

Second-order asymptotics for source coding, dense coding and pure-state entanglement conversions

Nilanjana Datta and Felix Leditzky

*Statistical Laboratory, Centre for Mathematical Sciences, University of Cambridge,
Wilberforce Road, Cambridge CB3 0WA, United Kingdom*

March 26, 2015

Abstract

We introduce two variants of the information spectrum relative entropy defined by Tomamichel and Hayashi [47] which have the particular advantage of satisfying the data-processing inequality, i.e. monotonicity under quantum operations. This property allows us to obtain one-shot bounds for various information-processing tasks in terms of these quantities. Moreover, these relative entropies have a second order asymptotic expansion, which in turn yields tight second order asymptotics for optimal rates of these tasks in the i.i.d. setting. The tasks studied in this paper are fixed-length quantum source coding, noisy dense coding, entanglement concentration, pure-state entanglement dilution, and transmission of information through a classical-quantum channel. In the latter case, we retrieve the second order asymptotics obtained by Tomamichel and Tan [48]. Our results also yield the known second order asymptotics of fixed-length classical source coding derived by Hayashi [19]. The second order asymptotics of entanglement concentration and dilution provide a refinement of the *inefficiency* of these protocols - a quantity which, in the case of entanglement dilution, was studied by Harrow and Lo [16]. We prove how the discrepancy between the optimal rates of these two processes in the second order implies the irreversibility of entanglement concentration established by Kumagai and Hayashi [28]. In addition, the spectral divergence rates of the Information Spectrum Approach (ISA) can be retrieved from our relative entropies in the asymptotic limit. This enables us to directly obtain the more general results of the ISA from our one-shot bounds.

1 Introduction

Optimal rates of information-processing tasks such as storage and transmission of information, and manipulation of entanglement, are of fundamental importance in Information Theory. These rates were originally evaluated in the so-called asymptotic, i.i.d.¹ setting, in which it is assumed that the underlying resources (sources, channels or entangled states) employed in the tasks are available for asymptotically many uses, and that there are no correlations between their successive uses. The rates in this scenario are given in terms of entropic quantities obtainable from the relative entropy. It is, however, unrealistic to assume the availability of infinitely many copies of the required resources. In practice, we have finite resources and hence a fundamental problem of both theoretical and practical interest is to determine how quickly the behaviour of a finite system approaches that of its asymptotic limit.

The first step in this direction, from the standpoint of Information Theory, is to determine the second order asymptotics of optimal rates.² Interest in this was initiated in the classical

¹Here, i.i.d. is the standard acronym for “independent and identically distributed”.

²The precise meaning of the phrase “second order asymptotics” is elucidated in the following paragraph.

realm by Strassen [44], who evaluated the second order asymptotics for hypothesis testing and channel coding. In the last decade there has been a renewal of interest in the evaluation of second order asymptotics for other classical information theoretic tasks (see e.g. [19, 20, 29] and references therein) and, more recently, even in third-order asymptotics [27]. Moreover, the recent papers by Tomamichel and Hayashi [47] and Li [30] have introduced the study of second order asymptotics in Quantum Information Theory as well. The achievability parts of the second order asymptotics for the tasks studied in [47, 30] were later also obtained by Beigi and Gohari [3] via the collision relative entropy.

Let us explain what exactly is meant by the phrase “second order asymptotics”. Consider the familiar task of fixed-length quantum source coding. Schumacher [41] proved that for a memoryless, quantum information source characterized by a state ρ , the optimal rate of reliable data compression is given by its von Neumann entropy, $S(\rho)$. The criterion of reliability is that the error incurred in the compression-decompression scheme vanishes in the asymptotic limit, $n \rightarrow \infty$, where n denotes the number of copies (or uses) of the source. Let us now consider instead a finite number (n) of copies of the source and require that the error incurred in compressing its state $\rho^{\otimes n}$ is at most ε (for some $0 < \varepsilon < 1$). Suppose $m^{n,\varepsilon}(\rho)$ denotes the compression length, i.e. the minimum of the logarithm of the dimension of the compressed Hilbert space in this case. This quantity can be expanded as follows:

$$m^{n,\varepsilon}(\rho) = an + b\sqrt{n} + \mathcal{O}(\log n) \quad (1)$$

Here, the coefficient a of the leading term constitutes the first order asymptotics of the compression length. As expected, it turns out to be the optimal rate in the asymptotic limit, i.e. the von Neumann entropy of the source. The second order asymptotics is given by the coefficient b , and is a function of both the error threshold ε and the state ρ . Determining the second order asymptotics comprises the evaluation of the coefficient b .

Theorem 5.8(i) of Section 5 gives an explicit expression for the coefficient b in the case of fixed-length (visible) quantum source coding. In Figure 1 we plot $(an + b\sqrt{n})/n$ against n for a memoryless quantum information source which emits the (mutually non-orthogonal) pure states $|0\rangle$ and $|+\rangle$ with equal probability, for three different values of the error threshold ε . This exhibits how the rate of data compression converges to its asymptotically optimal value.

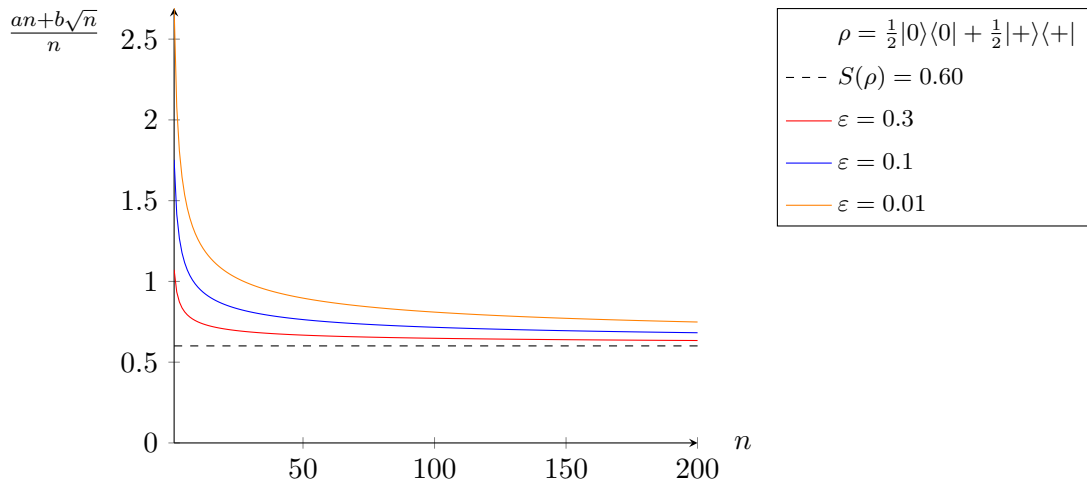


Figure 1: Plot of $\frac{an + b\sqrt{n}}{n}$ for the source $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|$.

In this paper we study the second order asymptotics of various information-processing tasks: fixed-length quantum source coding, noisy dense coding, entanglement concentration, pure-state

entanglement dilution, and transmission of information through a classical-quantum channel. For each task we consider the n -copy case, where n denotes the number of copies of the relevant resource (source, entangled state or channel) employed in the protocol, ε denotes the error threshold, and $m^{n,\varepsilon}(\rho)$ denotes the characteristic quantity of the protocol (e.g. the minimum compression length in the case of source coding). We arrive at an expression of the form (1) for $m^{n,\varepsilon}(\rho)$ – which in this case is a quantity from which the optimal asymptotic rate R of the protocol is obtained through the relation

$$R = \lim_{\varepsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} m^{n,\varepsilon}(\rho).$$

For each of the tasks studied, the coefficient a turns out to be the entropic quantity characterizing R . Moreover, the coefficient b is proportional to $\Phi^{-1}(\varepsilon)$, where Φ^{-1} denotes the inverse of the cumulative distribution function of the standard normal distribution, and the constant of proportionality depends on the underlying resource (the latter is often called the *dispersion* or *information variance*). This form of b is a feature of all results on second order asymptotics and stems from the Berry-Esseen theorem [13] – a refinement of the central limit theorem which takes into account the rate of convergence of a distribution to a standard normal distribution.

Two mathematical quantities play key roles in the derivation of our results. These are variants of the information spectrum relative entropy defined by Tomamichel and Hayashi [47], but have the particular advantage of satisfying the data-processing inequality. For a state ρ and a positive semi-definite operator σ , we denote them as $\underline{D}_s^\varepsilon(\rho||\sigma)$ and $\overline{D}_s^\varepsilon(\rho||\sigma)$ (where $0 < \varepsilon < 1$) and refer to them simply as *information spectrum relative entropies*³. These notations and nomenclatures stem from the fact that for any arbitrary sequence of states $\hat{\rho} := \{\rho_n\}_{n \in \mathbb{N}}$ and positive semi-definite operators $\hat{\sigma} := \{\sigma_n\}_{n \in \mathbb{N}}$ such that ρ_n and σ_n are defined on the Hilbert space $\mathcal{H}^{\otimes n}$ for each $n \in \mathbb{N}$, the following relations hold:

$$\lim_{\varepsilon \rightarrow 0} \liminf_{n \rightarrow \infty} \frac{1}{n} \underline{D}_s^\varepsilon(\rho_n||\omega_n) = \underline{D}(\hat{\rho}||\hat{\omega}) \quad \text{and} \quad \lim_{\varepsilon \rightarrow 0} \limsup_{n \rightarrow \infty} \frac{1}{n} \overline{D}_s^\varepsilon(\rho_n||\omega_n) = \overline{D}(\hat{\rho}||\hat{\sigma}), \quad (2)$$

where $\underline{D}(\hat{\rho}||\hat{\omega})$ and $\overline{D}(\hat{\rho}||\hat{\sigma})$ are the inf- and sup- spectral divergence rates of the so-called quantum Information Spectrum Approach (ISA) (see Definition 4.11). The ISA provides a unifying mathematical framework for obtaining asymptotic rate formulae for various different tasks in information theory. The power of the approach lies in the fact that it does not rely on any particular structure or property of the resources used in the tasks. It was introduced by Han and Verdu [15] in classical Information Theory, and generalized to the quantum setting by Hayashi, Nagaoka and Ogawa [18, 21, 33, 37].

The information spectrum relative entropies, $\underline{D}_s^\varepsilon(\rho||\sigma)$ and $\overline{D}_s^\varepsilon(\rho||\sigma)$, can also be related to other relative entropies which arise in one-shot information theory (see [38, 26, 9, 45, 10, 32] and references therein), e.g. the hypothesis testing relative entropy $D_H^\varepsilon(\rho||\sigma)$ [49], and the smooth max-relative entropy $D_{\max}^\varepsilon(\rho||\sigma)$ [9]. In fact, one can prove that all these relative entropies are equivalent in the sense that upper and lower bounds to any one of them can be obtained in terms of any one of the others, modulo terms which depend only on the (smoothing) parameter ε . These equivalences prove very useful. In particular, the bounds on the information spectrum relative entropy in terms of $D_H^\varepsilon(\rho||\sigma)$ directly yield second order asymptotic expansions for $\underline{D}_s^\varepsilon(\rho||\sigma)$ and $\overline{D}_s^\varepsilon(\rho||\sigma)$ via the second order asymptotic expansion for $D_H^\varepsilon(\rho||\sigma)$, which has been derived by Tomamichel and Hayashi in [47].

In addition, as in the case of the usual relative entropy, one can derive other entropic quantities, namely, entropy, conditional entropy and mutual information, from the information

³ To avoid confusion, we denote the information spectrum relative entropy defined in [47] by $D_s^\varepsilon(\rho||\sigma)$.

spectrum relative entropies. For each of the information-processing tasks considered in this paper, we obtain one-shot bounds in terms of quantities derived from the information spectrum relative entropies. The second order expansions of these quantities then directly yield tight second order asymptotics for optimal rates of the corresponding tasks in the i.i.d. setting.

Finally, the relations (2) enable us to directly obtain the more general results of the ISA, for each of the tasks considered, from our one-shot bounds. For example, our bounds for one-shot fixed-length source coding yields the optimal data compression limit for a general (i.e. not necessarily memoryless) quantum information source.

2 Overview of results

Here we summarize our main contributions and give pointers to the relevant theorems.

- We define the information spectrum relative entropies in Definition 4.1 as a variant of a previously introduced relative entropy [47], and furthermore define quantities derived from them in Definition 4.4. These quantities all depend on a parameter $0 < \varepsilon < 1$.
- We prove the data-processing inequalities and other properties of the information spectrum relative entropies in Proposition 4.3. We also show in Proposition 4.7 that the information spectrum relative entropies are equivalent to the hypothesis testing relative entropy and the smooth max-relative entropy, in the sense that these quantities are bounded by each other.
- Using their equivalences with the hypothesis testing relative entropy, and the second order asymptotic expansion for the latter [47], we obtain second order asymptotic expansions for the information spectrum relative entropies in Proposition 4.9.
- In Proposition 4.12 we prove that the information spectrum relative entropies reduce to the spectral divergence rates of the ISA in the asymptotic limit, when the parameter ε is taken to zero.
- We obtain one-shot bounds for the following information-processing tasks in terms of quantities derived from the information spectrum relative entropies. In each case the parameter ε plays the role of the error threshold allowed in the protocol.
 1. Quantum fixed-length source coding [Theorem 5.5].
 2. Noisy dense coding [Theorem 5.10].
 3. Entanglement concentration [Theorem 5.14].
 4. Pure-state entanglement dilution [Theorem 5.17].
 5. Classical-quantum channel coding [Theorem 5.23].
- We obtain second order asymptotic expansions for the optimal rates of the above tasks in the i.i.d. setting in Theorems 5.8, 5.11, 5.15, 5.18 and Proposition 5.24 respectively.

In particular, Theorem 5.8(i) gives the second order expansion for fixed-length visible quantum source coding. We also obtain asymptotic upper and lower bounds on the minimal compression length in the blind setting, stated in Theorem 5.8(ii). The distinction between visible and the blind source coding is elaborated in Section 5.1.1.
- Even though the leading order terms for the optimal rates for entanglement concentration and dilution are identical (and given by the entropy of entanglement), there is a difference

in their second order terms. Explicit evaluation of these terms lead to a refinement of the *inefficiency* of these protocols. In the case of entanglement dilution, the latter quantity (studied by Harrow and Lo [16]) was introduced as a measure of the amount of entanglement wasted (or lost) in the dilution process. More precisely, in [16] it was proved that the number of ebits needed to create n copies of a desired bipartite pure state ψ_{AB} with entropy of entanglement E was of the form $En + \Omega(\sqrt{n})$. We prove that the number of ebits can, in fact, be expressed in the form $En + b\sqrt{n} + \mathcal{O}(\log n)$, and we evaluate the coefficient b explicitly.

We also show how the irreversibility of entanglement concentration, established by Kümargai and Hayashi [28], can be proved using the discrepancy between the asymptotic expansions for distillable entanglement and entanglement cost in the second order (\sqrt{n}).

- Finally, in Proposition 6.2, we recover the known expressions for optimal rates in the case of arbitrary resources as obtained by the Information Spectrum Approach.

The paper is organized as follows. In the next section, we introduce necessary notation and definitions. The rest of the paper proceeds in the order of the results mentioned above. We end with a conclusion that summarizes our results and points to open questions for future research.

3 Mathematical preliminaries

For a Hilbert space \mathcal{H} , let $\mathcal{B}(\mathcal{H})$ denote the algebra of linear operators acting on \mathcal{H} , and let $\mathcal{P}(\mathcal{H})$ denote the set of positive semi-definite operators on \mathcal{H} . Further, let $\mathcal{D}(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) \mid \text{Tr } \rho = 1\}$ and $\mathcal{D}_{\leq}(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) \mid \text{Tr } \rho \leq 1\}$ denote the set of states (density matrices) and subnormalized states on \mathcal{H} respectively. For a state $\rho \in \mathcal{D}(\mathcal{H})$, the von Neumann entropy $S(\rho)$ is defined as $S(\rho) = -\text{Tr } \rho \log \rho$. Here and henceforth, all logarithms are taken to base 2. Unless otherwise stated, we assume all Hilbert spaces to be finite-dimensional. Let $\mathbb{1} \in \mathcal{P}(\mathcal{H})$ denote the identity operator on \mathcal{H} , and $\text{id} : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$ the identity map on operators on \mathcal{H} . For a pure state $|\psi\rangle$, we denote the corresponding projector by $\psi \equiv |\psi\rangle\langle\psi|$. For a completely positive, trace-preserving (CPTP) map $\Lambda : \mathcal{D}(\mathcal{H}_A) \rightarrow \mathcal{D}(\mathcal{H}_{A'})$, we also use the shorthand notation $\Lambda^{A \rightarrow A'}$.

For self-adjoint operators $A, B \in \mathcal{B}(\mathcal{H})$, let $\{A \geq B\}$ denote the spectral projection of the difference operator $A - B$ corresponding to the interval $[0, +\infty)$; the spectral projections $\{A > B\}$, $\{A \leq B\}$ and $\{A < B\}$ are defined in a similar way. We also define $A_+ = PAP$ where $P := \{A \geq 0\}$ for any self-adjoint operator $A \in \mathcal{B}(\mathcal{H})$. The following lemmas are used in our proofs:

Lemma 3.1. [37] *Let $A, B \geq 0$ and $0 \leq P \leq \mathbb{1}$ be an arbitrary operator, then*

$$\text{Tr}[\{A \geq B\}(A - B)] \geq \text{Tr}[P(A - B)],$$

and the same assertion holds for $\{A > B\}$.

Lemma 3.2. [5] *Let $A, B \geq 0$ and Λ be a CPTP map. Then*

$$\text{Tr}[(\Lambda(A) - \Lambda(B))\{\Lambda(A) > \Lambda(B)\}] \leq \text{Tr}[(A - B)\{A > B\}].$$

Lemma 3.3. [5] *Let $\rho \in \mathcal{D}_{\leq}(\mathcal{H})$ and $\sigma \in \mathcal{P}(\mathcal{H})$. Then for any $\gamma \in \mathbb{R}$,*

$$\text{Tr}[\{\rho \geq 2^{-\gamma}\sigma\}\sigma] \leq 2^{\gamma}.$$

For the convenience of the reader, we recall the definitions of the most important distance measures and state their relations [46]:

Definition 3.4. Let $\rho, \sigma \in \mathcal{D}_{\leq}(\mathcal{H})$ be subnormalized states, then:

- (i) The *generalized fidelity* $F(\rho, \sigma)$ of ρ and σ is defined by

$$F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1 + \sqrt{(1 - \text{Tr } \rho)(1 - \text{Tr } \sigma)}.$$

- (ii) The *purified distance* $P(\rho, \sigma)$ is defined by

$$P(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)^2}$$

and constitutes a metric on $\mathcal{D}_{\leq}(\mathcal{H})$, i.e. it satisfies the triangle inequality.

- (iii) The *generalized trace distance* $d(\rho, \sigma)$ is defined by

$$d(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1 + \frac{1}{2}|\text{Tr } \rho - \text{Tr } \sigma|$$

and constitutes a metric on $\mathcal{D}_{\leq}(\mathcal{H})$.

If at least one of the subnormalized states ρ and σ is normalized, the generalized fidelity reduces to the usual fidelity, i.e. $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1 = \text{Tr}(\sqrt{\rho}\sigma\sqrt{\rho})^{\frac{1}{2}}$. If both ρ and σ are normalized, the generalized trace distance also reduces to the usual trace distance, $d(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1$. \diamond

Lemma 3.5. [45] For $\rho, \sigma \in \mathcal{D}_{\leq}(\mathcal{H})$ we have the following bounds:

$$d(\rho, \sigma) \leq P(\rho, \sigma) \leq \sqrt{2d(\rho, \sigma)}$$

The following entropic quantities play a key role in second order asymptotic expansions:

Definition 3.6. For $\rho \in \mathcal{D}(\mathcal{H})$ and $\sigma \in \mathcal{P}(\mathcal{H})$, the *quantum relative entropy* $D(\rho\|\sigma)$ is defined as

$$D(\rho\|\sigma) := \begin{cases} \text{Tr}[\rho(\log \rho - \log \sigma)] & \text{supp } \rho \subseteq \text{supp } \sigma \\ \infty & \text{else.} \end{cases}$$

The *quantum information variance* $V(\rho\|\sigma)$ is defined as

$$V(\rho\|\sigma) := \text{Tr}[\rho(\log \rho - \log \sigma)^2] - D(\rho\|\sigma)^2,$$

and we set

$$\mathfrak{s}(\rho\|\sigma) := \sqrt{V(\rho\|\sigma)}. \tag{3}$$

\diamond

The inverse of the cumulative distribution function (cdf) of a standard normal random variable is defined by

$$\Phi^{-1}(\varepsilon) := \sup\{z \in \mathbb{R} \mid \Phi(z) \leq \varepsilon\},$$

where $\Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^z e^{-t^2/2} dt$. We frequently make use of the following lemma:

Lemma 3.7. Let $\varepsilon > 0$, then

$$\sqrt{n} \Phi^{-1} \left(\varepsilon \pm \frac{1}{\sqrt{n}} \right) = \sqrt{n} \Phi^{-1}(\varepsilon) \pm (\Phi^{-1})'(\xi)$$

for some ξ with $|\xi - \varepsilon| \leq \frac{1}{\sqrt{n}}$.

Proof. We make the following general observation: Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be a continuously differentiable function. Then by Taylor's theorem we can write

$$f \left(x \pm \frac{1}{\sqrt{n}} \right) = f(x) \pm \frac{1}{\sqrt{n}} f'(\xi) \tag{4}$$

for some $\xi \in \left[x - \frac{1}{\sqrt{n}}, x \right]$ in the case ‘−’ and $\xi \in \left[x, x + \frac{1}{\sqrt{n}} \right]$ in the case ‘+’. Applying (4) to $\sqrt{n} \Phi^{-1} \left(\varepsilon \pm \frac{1}{\sqrt{n}} \right)$ yields the claim. \square

4 Information spectrum relative entropies

4.1 Definitions and mathematical properties

The central quantities of this paper are the information spectrum relative entropies $\underline{D}_s^\varepsilon(\rho\|\sigma)$ and $\overline{D}_s^\varepsilon(\rho\|\sigma)$, which we now define.

Definition 4.1. For $\rho \in \mathcal{D}(\mathcal{H})$, $\sigma \in \mathcal{P}(\mathcal{H})$ and $\varepsilon \in (0, 1)$, the *information spectrum relative entropies* are defined as

$$\begin{aligned}\underline{D}_s^\varepsilon(\rho\|\sigma) &:= \sup\{\gamma \mid \text{Tr}[(\rho - 2^\gamma \sigma)\{\rho > 2^\gamma \sigma\}] \geq 1 - \varepsilon\} \\ \overline{D}_s^\varepsilon(\rho\|\sigma) &:= \inf\{\gamma \mid \text{Tr}[(\rho - 2^\gamma \sigma)\{\rho > 2^\gamma \sigma\}] \leq \varepsilon\}.\end{aligned}\quad \diamond$$

These relative entropies are one-shot generalizations of the spectral divergences used in the ISA to quantum information theory. In Section 4.4 these generalizations are discussed in detail.

Note furthermore, that the information spectrum relative entropies as defined in Definition 4.1 are variants of the definition introduced by Tomamichel and Hayashi [47]:

$$D_s^\varepsilon(\rho\|\sigma) := \sup\{\gamma \mid \text{Tr}[\rho\{\rho \leq 2^\gamma \sigma\}] \leq \varepsilon\}. \quad (5)$$

Our definitions have the advantage of satisfying the data processing inequality, as shown in Proposition 4.3(iii). First, we prove the following lemma which implies that the supremum and infimum in Definition 4.1 are attained.

Lemma 4.2.

- (i) Let $A(\gamma) \in \mathcal{B}(\mathcal{H})$ be a Hermitian operator continuously depending on a real parameter γ (with respect to the operator norm). Then the function $\gamma \mapsto \text{Tr}(A(\gamma))_+$ is continuous.
- (ii) Let A, B be Hermitian operators with $A \leq B$, then $A_+ \leq B_+$.
- (iii) The function $\gamma \mapsto \text{Tr}(\rho - 2^\gamma \sigma)_+$ is continuous and strictly decreasing.
- (iv) The supremum and infimum in Definition 4.1 are attained.

Proof. (i) First, we observe that the trace of the positive part of a Hermitian operator is the sum of its non-negative eigenvalues, the eigenvalues being the roots of the characteristic polynomial. Since the determinant is a continuous function with respect to the operator norm on $\mathcal{B}(\mathcal{H})$, the coefficients of the characteristic polynomial of $A(\gamma)$ continuously depend on γ , and by factorizing the polynomial into linear factors we see that this carries over to the roots. Composing the sum over the roots with the continuous maximum function $\max(\cdot, 0)$, we finally obtain that the function $\gamma \mapsto \text{Tr}(A(\gamma))_+$ is a composition of continuous functions and thus continuous itself.

(ii) The claim $A_+ \leq B_+$ is equivalent to $\langle n|A_+|n\rangle \leq \langle n|B_+|n\rangle$ for all n where $\{|n\rangle\}$ is an orthonormal basis for \mathcal{H} . Let $\{|i_A\rangle\}$ be the eigenbasis of A and consider first a basis vector $|i_A\rangle$ corresponding to a non-negative eigenvalue. Then we have

$$\begin{aligned}\langle i_A|A_+|i_A\rangle &= \langle i_A|A|i_A\rangle \\ &\leq \langle i_A|B|i_A\rangle \\ &\leq \langle i_A|B_+|i_A\rangle,\end{aligned}$$

where the first inequality follows from the assumption $A \leq B$ and the second inequality follows from the trivial fact that $C \leq C_+$ for any operator C .

Conversely, let $|i_A\rangle$ be an eigenvector corresponding to a negative eigenvalue. Then

$$\langle i_A|A_+|i_A\rangle = 0 \leq \langle i_A|B_+|i_A\rangle$$

since B_+ is a positive operator by definition. In summary, we have $\langle i_A | A_+ | i_A \rangle \leq \langle i_A | B_+ | i_A \rangle$ for all i , which yields the claim.

(iii) Since $\gamma \mapsto \rho - 2^\gamma \sigma$ is continuous, the function $\gamma \mapsto \text{Tr}(\rho - 2^\gamma \sigma)_+$ is continuous by (i). Furthermore, we clearly have $\rho - 2^\gamma \sigma < \rho - 2^{\gamma'} \sigma$ for $\gamma' < \gamma$, and hence $\text{Tr}(\rho - 2^\gamma \sigma)_+ < \text{Tr}(\rho - 2^{\gamma'} \sigma)_+$ by (ii).

(iv) Since $\lim_{\gamma \rightarrow -\infty} \text{Tr}(\rho - 2^\gamma \sigma)_+ = \text{Tr}(\rho) = 1$ and $\lim_{\gamma \rightarrow \infty} \text{Tr}(\rho - 2^\gamma \sigma)_+ = 0$, we infer by (iii) and the intermediate value theorem that the supremum in the definition of $\underline{D}_s^\varepsilon(\rho \| \sigma)$ as well as the infimum in the definition of $\overline{D}_s^\varepsilon(\rho \| \sigma)$ are attained. \square

We are now ready to record a series of properties of the information spectrum relative entropies:

Proposition 4.3. *Let $\varepsilon \in (0, 1)$, $\rho \in \mathcal{D}(\mathcal{H})$ and $\sigma \in \mathcal{P}(\mathcal{H})$. Then the following properties hold:*

- (i) $\underline{D}_s^\varepsilon(\rho \| \sigma) \leq D_s^\varepsilon(\rho \| \sigma)$
- (ii) $\underline{D}_s^\varepsilon(\rho \| \sigma) = \overline{D}_s^{1-\varepsilon}(\rho \| \sigma)$
- (iii) *Data processing inequality: For any CPTP map Λ , we have*

$$\begin{aligned} \underline{D}_s^\varepsilon(\rho \| \sigma) &\geq \underline{D}_s^\varepsilon(\Lambda(\rho) \| \Lambda(\sigma)) \\ \overline{D}_s^\varepsilon(\rho \| \sigma) &\geq \overline{D}_s^\varepsilon(\Lambda(\rho) \| \Lambda(\sigma)). \end{aligned}$$

- (iv) *Monotonicity in ε : Let $\varepsilon' \geq \varepsilon$, then*

$$\begin{aligned} \underline{D}_s^\varepsilon(\rho \| \sigma) &\leq \underline{D}_s^{\varepsilon'}(\rho \| \sigma) \\ \overline{D}_s^{\varepsilon'}(\rho \| \sigma) &\leq \overline{D}_s^\varepsilon(\rho \| \sigma). \end{aligned}$$

- (v) *Let $\sigma' \geq 0$ with $\sigma \leq \sigma'$, then $\underline{D}_s^\varepsilon(\rho \| \sigma) \geq \underline{D}_s^\varepsilon(\rho \| \sigma')$.*
- (vi) *Let $c > 0$, then $\underline{D}_s^\varepsilon(\rho \| c\sigma) = \underline{D}_s^\varepsilon(\rho \| \sigma) - \log c$.*
- (vii) *Let $\delta > 0$ and $\rho' \in \mathcal{D}(\mathcal{H})$ with $d(\rho, \rho') \leq \delta$, then $\underline{D}_s^\varepsilon(\rho' \| \sigma) \leq \underline{D}_s^{\varepsilon+\delta}(\rho \| \sigma)$.*

Proof. (i) Let $\gamma = \underline{D}_s^\varepsilon(\rho \| \sigma)$. Then by the definition of $\underline{D}_s^\varepsilon(\rho \| \sigma)$ we have

$$\begin{aligned} 1 - \varepsilon &= \text{Tr}[(\rho - 2^\gamma \sigma)\{\rho > 2^\gamma \sigma\}] \\ &\leq \text{Tr}[\rho\{\rho > 2^\gamma \sigma\}]. \end{aligned}$$

Hence,

$$\begin{aligned} \text{Tr}[\rho\{\rho \leq 2^\gamma \sigma\}] &= \text{Tr} \rho - \text{Tr}[\rho\{\rho > 2^\gamma \sigma\}] \\ &\leq \text{Tr} \rho - (1 - \varepsilon) \\ &= \varepsilon, \end{aligned}$$

since $\text{Tr} \rho = 1$ by assumption. Therefore, γ is feasible for $D_s^\varepsilon(\rho \| \sigma)$ and consequently, from (5) it follows that

$$D_s^\varepsilon(\rho \| \sigma) \geq \gamma = \underline{D}_s^\varepsilon(\rho \| \sigma),$$

which yields the claim.

- (ii) Let $\gamma = \overline{D}_s^{1-\varepsilon}(\rho \| \sigma)$. Then by the definition of $\overline{D}_s^{1-\varepsilon}(\rho \| \sigma)$, we have

$$\text{Tr}(\rho - 2^\gamma \sigma)_+ = 1 - \varepsilon.$$

Hence, γ is feasible for $\underline{D}_s^\varepsilon(\rho\|\sigma)$, and we obtain

$$\underline{D}_s^\varepsilon(\rho\|\sigma) \geq \gamma = \overline{D}_s^{1-\varepsilon}(\rho\|\sigma).$$

Assume now that

$$\gamma = \overline{D}_s^{1-\varepsilon}(\rho\|\sigma) = \underline{D}_s^\varepsilon(\rho\|\sigma) - \delta$$

for some $\delta > 0$, i.e. $\overline{D}_s^{1-\varepsilon}(\rho\|\sigma) < \underline{D}_s^\varepsilon(\rho\|\sigma)$. By the monotonicity of $\alpha \mapsto \text{Tr}(\rho - 2^\alpha \sigma)_+$, we have

$$\text{Tr}(\rho - 2^\gamma \sigma)_+ > 1 - \varepsilon.$$

On the other hand, $\text{Tr}(\rho - 2^\gamma \sigma)_+ = 1 - \varepsilon$ by definition of $\overline{D}_s^{1-\varepsilon}(\rho\|\sigma)$. This leads to a contradiction, yielding $\underline{D}_s^\varepsilon(\rho\|\sigma) = \overline{D}_s^{1-\varepsilon}(\rho\|\sigma)$.

(iii) Let $\gamma = \underline{D}_s^\varepsilon(\Lambda(\rho)\|\Lambda(\sigma))$. Then Lemma 3.2 implies that

$$\text{Tr}(\rho - 2^\gamma \sigma)_+ \geq \text{Tr}(\Lambda(\rho) - 2^\gamma \Lambda(\sigma))_+ = 1 - \varepsilon.$$

Hence, γ is feasible for $\underline{D}_s^\varepsilon(\rho\|\sigma)$, and we obtain

$$\underline{D}_s^\varepsilon(\rho\|\sigma) \geq \gamma = \underline{D}_s^\varepsilon(\Lambda(\rho)\|\Lambda(\sigma)).$$

Similarly, let $\gamma = \overline{D}_s^\varepsilon(\rho\|\sigma)$. Then

$$\varepsilon = \text{Tr}(\rho - 2^\gamma \sigma)_+ \geq \text{Tr}(\Lambda(\rho) - 2^\gamma \Lambda(\sigma))_+$$

by Lemma 3.2. Hence, γ is feasible for $\overline{D}_s^\varepsilon(\Lambda(\rho)\|\Lambda(\sigma))$, and we obtain

$$\overline{D}_s^\varepsilon(\Lambda(\rho)\|\Lambda(\sigma)) \leq \gamma = \overline{D}_s^\varepsilon(\rho\|\sigma).$$

(iv) Let $\gamma = \underline{D}_s^\varepsilon(\rho\|\sigma)$, then

$$\text{Tr}[\{\rho > 2^\gamma \sigma\}(\rho - 2^\gamma \sigma)] = 1 - \varepsilon \geq 1 - \varepsilon'.$$

Hence, γ is feasible for $\underline{D}_s^{\varepsilon'}(\rho\|\sigma)$, and consequently, $\underline{D}_s^{\varepsilon'}(\rho\|\sigma) \geq \gamma = \underline{D}_s^\varepsilon(\rho\|\sigma)$.

Similarly, let $\gamma = \overline{D}_s^\varepsilon(\rho\|\sigma)$. Then

$$\text{Tr}(\rho - 2^\gamma \sigma)_+ = \varepsilon \leq \varepsilon',$$

and hence, γ is feasible for $\overline{D}_s^{\varepsilon'}(\rho\|\sigma)$, and we obtain $\overline{D}_s^{\varepsilon'}(\rho\|\sigma) \leq \gamma = \overline{D}_s^\varepsilon(\rho\|\sigma)$.

(v) Let $\gamma = \underline{D}_s^\varepsilon(\rho\|\sigma')$ and $Q = \{\rho > 2^\gamma \sigma'\}$, then we compute:

$$\begin{aligned} 1 - \varepsilon &= \text{Tr}[Q(\rho - 2^\gamma \sigma')] \\ &= \text{Tr} Q \rho - 2^\gamma \text{Tr} Q \sigma' \\ &\leq \text{Tr} Q \rho - 2^\gamma \text{Tr} Q \sigma \\ &\leq \text{Tr}(\rho - 2^\gamma \sigma)_+ \end{aligned}$$

where the first inequality follows from $\sigma \leq \sigma'$ and the second inequality follows from Lemma 3.1.

Hence, γ is feasible for $\underline{D}_s^\varepsilon(\rho\|\sigma)$ and we obtain $\underline{D}_s^\varepsilon(\rho\|\sigma) \geq \underline{D}_s^\varepsilon(\rho\|\sigma')$.

(vi) Let $\gamma = \underline{D}_s^\varepsilon(\rho\|c\sigma)$ for $c > 0$, then

$$1 - \varepsilon = \text{Tr}(\rho - 2^\gamma c\sigma)_+ = \text{Tr}(\rho - 2^{\gamma+\log c} \sigma)_+$$

and hence,

$$\underline{D}_s^\varepsilon(\rho\|\sigma) \geq \gamma + \log c = \underline{D}_s^\varepsilon(\rho\|c\sigma) + \log c.$$

Conversely, let $\gamma = \underline{D}_s^\varepsilon(\rho\|\sigma)$. Then

$$1 - \varepsilon = \text{Tr}(\rho - 2^\gamma \sigma)_+ = \text{Tr}(\rho - 2^{\gamma - \log c} c\sigma)_+,$$

and hence,

$$\underline{D}_s^\varepsilon(\rho\|c\sigma) \geq \gamma - \log c = \underline{D}_s^\varepsilon(\rho\|\sigma) - \log c,$$

which proves the claim.

(vii) Let $\gamma = \underline{D}_s^\varepsilon(\rho'\|\sigma)$ and $Q = \{\rho' \geq 2^\gamma \sigma\}$. Then

$$\begin{aligned} 1 - \varepsilon &= \text{Tr}[(\rho' - 2^\gamma \sigma)Q] \\ &= \text{Tr}[(\rho' - \rho)Q] + \text{Tr}[(\rho - 2^\gamma \sigma)Q] \\ &\leq \text{Tr}(\rho' - \rho)_+ + \text{Tr}(\rho - 2^\gamma \sigma)_+ \\ &\leq \delta + \text{Tr}(\rho - 2^\gamma \sigma)_+, \end{aligned}$$

where the first inequality follows from Lemma 3.1 and the second inequality follows from the fact [45] that

$$d(\rho, \rho') = \text{Tr}(\rho - \rho')_+ \leq \delta$$

by assumption. This proves the claim. \square

Remark. Proposition 4.3(ii) shows that we only need to focus on one of the information spectrum relative entropies (we choose $\underline{D}_s^\varepsilon(\rho\|\sigma)$ without loss of generality). However, given their close relationship to the quantum spectral inf- and sup divergence (Section 4.4), we note that it is useful to keep the two alternative definitions in Definition 4.1. \diamond

Children entropies of the information spectrum relative entropies

The quantum relative entropy acts as a parent quantity for other entropic quantities:

- the von Neumann entropy $S(\rho) = -D(\rho\|\mathbb{1})$
- the quantum conditional entropy $S(A|B)_\rho = -D(\rho_{AB}\|\mathbb{1}_A \otimes \rho_B)$
- the quantum mutual information $I(A : B)_\rho = \min_{\sigma_B} D(\rho_{AB}\|\rho_A \otimes \sigma_B)$

This motivates us to define the following information spectrum entropies:

Definition 4.4. Let $\varepsilon \in (0, 1)$ and $\omega \in \mathcal{D}(\mathcal{H})$, $\sigma_B \in \mathcal{D}(\mathcal{H}_B)$, $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ be states. Then we define:

(i) the *information spectrum entropies*

$$\begin{aligned} \underline{H}_s^\varepsilon(\omega) &:= -\overline{D}_s^\varepsilon(\omega\|\mathbb{1}) \\ \overline{H}_s^\varepsilon(\omega) &:= -\underline{D}_s^\varepsilon(\omega\|\mathbb{1}) \end{aligned}$$

(ii) the *information spectrum conditional entropies*

$$\begin{aligned} \underline{H}_s^\varepsilon(A|B)_\rho &:= -\overline{D}_s^\varepsilon(\rho_{AB}\|\mathbb{1}_A \otimes \rho_B) \\ \overline{H}_s^\varepsilon(A|B)_\rho &:= -\underline{D}_s^\varepsilon(\rho_{AB}\|\mathbb{1}_A \otimes \rho_B) \end{aligned}$$

(iii) the *information spectrum mutual informations*

$$\begin{aligned}\underline{I}_s^\varepsilon(A : B)_\rho &:= \min_{\sigma_B} \underline{D}_s^\varepsilon(\rho_{AB} \| \rho_A \otimes \sigma_B) \\ \overline{I}_s^\varepsilon(A : B)_\rho &= \min_{\sigma_B} \overline{D}_s^\varepsilon(\rho_{AB} \| \rho_A \otimes \sigma_B)\end{aligned}\quad \diamond$$

Note that in Definition 4.4, (i) and (ii) the occurrence of the minus sign is the reason for changing the upper bar to a lower bar and vice versa. In Section 5 these quantities arise in one-shot bounds for operational tasks.

The information spectrum conditional entropies satisfy the following interesting property under local operations and classical communication (LOCC):

Lemma 4.5. *Let $\sigma_{AB} := \Lambda(\psi_{AB})$ where Λ denotes any LOCC operation and $\psi_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ is a bipartite pure state. Then the following inequality holds:*

$$\overline{H}_s^\varepsilon(A|B)_\psi \leq \overline{H}_s^\varepsilon(A|B)_\sigma$$

Proof. By definition, we have $-\overline{H}_s^\varepsilon(A|B)_\psi = \underline{D}_s^\varepsilon(\psi_{AB} \| \mathbb{1}_A \otimes \psi_B)$, and furthermore,

$$\begin{aligned}-\overline{H}_s^\varepsilon(A|B)_\sigma &= \underline{D}_s^\varepsilon(\sigma_{AB} \| \mathbb{1}_A \otimes \sigma_B) \\ &= \underline{D}_s^\varepsilon(\Lambda(\psi_{AB}) \| \mathbb{1}_A \otimes \sigma_B).\end{aligned}$$

However, by a result of Lo and Popescu [31], the action of the LOCC map Λ on the pure state ψ_{AB} can be expressed as follows:

$$\sigma_{AB} = \Lambda(\psi_{AB}) = \sum_j (U_j \otimes K_j) \psi_{AB} (U_j^\dagger \otimes K_j^\dagger),$$

where the U_j are unitary operators and K_j are operators such that $\sum_j K_j^\dagger K_j = \mathbb{1}_B$. Consequently, using the cyclicity of the trace we obtain

$$\sigma_B = \text{Tr}_A \sigma_{AB} = \sum_j K_j \psi_B K_j^\dagger. \quad (6)$$

Further, for $\psi_B = \text{Tr}_A \psi_{AB}$, we have

$$\Lambda(\mathbb{1}_A \otimes \psi_B) = \mathbb{1}_A \otimes \sigma_B,$$

which can be seen as follows:

$$\begin{aligned}\Lambda(\mathbb{1}_A \otimes \psi_B) &= \sum_j U_j U_j^\dagger \otimes K_j \psi_B K_j^\dagger \\ &= \mathbb{1}_A \otimes \sum_j K_j \psi_B K_j^\dagger \\ &= \mathbb{1}_A \otimes \sigma_B,\end{aligned}$$

where the second identity follows from the unitarity of the operators U_j , and the last identity follows from (6). Hence,

$$\begin{aligned}-\overline{H}_s^\varepsilon(A|B)_\sigma &= \underline{D}_s^\varepsilon(\Lambda(\psi_{AB}) \| \mathbb{1}_A \otimes \sigma_B) \\ &= \underline{D}_s^\varepsilon(\Lambda(\psi_{AB}) \| \Lambda(\mathbb{1}_A \otimes \psi_B)) \\ &\leq \underline{D}_s^\varepsilon(\psi_{AB} \| \mathbb{1}_A \otimes \psi_B) \\ &= -\overline{H}_s^\varepsilon(A|B)_\psi,\end{aligned}$$

where the inequality follows from Proposition 4.3, (iii). \square

4.2 Relation to other relative entropies

In this section we prove that the information spectrum relative entropies are equivalent to the hypothesis testing relative entropies and the smooth max-relative entropy, which arise in one-shot information theory. This equivalence is in the sense that upper and lower bounds to any one of them can be obtained in terms of any one of the others, modulo terms which depend only on the (smoothing) parameter ε . Let us first recall the definitions of the hypothesis testing relative entropies and the smooth max-relative entropy:

Definition 4.6.

- (i) For $0 < \varepsilon < 1$ and $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, the *hypothesis testing relative entropy* $D_H^\varepsilon(\rho\|\sigma)$ is defined as

$$D_H^\varepsilon(\rho\|\sigma) := -\log \inf_{0 \leq Q \leq \mathbb{1}} \{\text{Tr } Q\sigma \mid \text{Tr } Q\rho \geq 1 - \varepsilon\}.$$

- (ii) For $\varepsilon > 0$, $\rho \in \mathcal{D}_\leq(\mathcal{H})$ and $\sigma \geq 0$, the *smooth max-relative entropy* $D_{\max}^\varepsilon(\rho\|\sigma)$ is defined as

$$D_{\max}^\varepsilon(\rho\|\sigma) := \min_{\bar{\rho} \in \mathcal{B}^\varepsilon(\rho)} \inf\{\gamma \mid \bar{\rho} \leq 2^\gamma \sigma\},$$

where $\mathcal{B}^\varepsilon(\rho) := \{\bar{\rho} \in \mathcal{D}_\leq(\mathcal{H}) \mid F(\bar{\rho}, \rho)^2 \geq 1 - \varepsilon^2\}$ is the ε -ball with respect to the purified distance $P(\rho, \sigma)$. \diamond

We prove the following relations between these relative entropies:

Proposition 4.7. *Let $0 < \varepsilon < 1$, $\delta, \eta > 0$, and $\rho, \sigma > 0$ with $\text{Tr } \rho \leq 1$. Then we obtain the following bounds:*

- (i) $D_H^{\varepsilon-\delta}(\rho\|\sigma) + \log \delta \leq \underline{D}_s^\varepsilon(\rho\|\sigma) \leq D_H^\varepsilon(\rho\|\sigma)$
- (ii) $D_H^{\varepsilon-\eta}(\rho\|\sigma) + \log \eta \leq \overline{D}_s^{1-\varepsilon}(\rho\|\sigma) \leq D_H^\varepsilon(\rho\|\sigma) + \delta$
- (iii) $D_{\max}^{\sqrt{8\varepsilon}}(\rho\|\sigma) \leq \overline{D}_s^\varepsilon(\rho\|\sigma) \leq D_{\max}^\varepsilon(\rho\|\sigma)$

Proof. (i) To prove the upper bound, let $Q := \{\rho > 2^\gamma \sigma\}$ where $\gamma = \underline{D}_s^\varepsilon(\rho\|\sigma) - \xi$ for some $\xi > 0$. Since

$$\text{Tr } \rho Q \geq \text{Tr}[(\rho - 2^\gamma \sigma)Q] \geq 1 - \varepsilon,$$

we see that Q is feasible for $D_H^\varepsilon(\rho\|\sigma)$. Hence,

$$\begin{aligned} \text{Tr } \sigma Q &= \text{Tr}[\sigma\{\rho > 2^\gamma \sigma\}] \\ &\leq 2^{-\gamma} \text{Tr}[\rho\{\rho > 2^\gamma \sigma\}] \\ &\leq 2^{-\gamma} \end{aligned}$$

since $\text{Tr } \rho \leq 1$. By the definition of $D_H^\varepsilon(\rho\|\sigma)$, we obtain

$$D_H^\varepsilon(\rho\|\sigma) \geq \gamma = \underline{D}_s^\varepsilon(\rho\|\sigma) - \xi,$$

and hence the lower bound.

Conversely, let $0 \leq Q \leq \mathbb{1}$ be optimal for $D_H^\varepsilon(\rho\|\sigma)$ and set $\mu = \log \delta + D_H^\varepsilon(\rho\|\sigma)$. Then

$$\begin{aligned} \text{Tr}(\rho - 2^\mu \sigma)_+ &\geq \text{Tr}[Q(\rho - 2^\mu \sigma)] \\ &= \text{Tr } Q\rho - 2^\mu \text{Tr } Q\sigma \\ &\geq 1 - (\varepsilon + \delta), \end{aligned}$$

where the first inequality follows from Lemma 3.1. Hence, μ is feasible for $\underline{D}_s^{\varepsilon+\delta}(\rho\|\sigma)$ and we obtain

$$\underline{D}_s^{\varepsilon+\delta}(\rho\|\sigma) \geq D_H^\varepsilon(\rho\|\sigma) + \log \delta.$$

(ii) We start with the upper bound. Let $\gamma = \overline{D}_s^{1-\varepsilon}(\rho\|\sigma) - \delta$ for some arbitrary $\delta > 0$ and set $Q := \{\rho \geq 2^\gamma \sigma\}$. We have $\text{Tr}[Q(\rho - 2^\gamma \sigma)] > 1 - \varepsilon$ by definition of $\overline{D}_s^{1-\varepsilon}(\rho\|\sigma)$, and hence,

$$\text{Tr } Q\rho \geq \text{Tr}[Q(\rho - 2^\gamma \sigma)] > 1 - \varepsilon.$$

Thus, Q is feasible for $D_H^\varepsilon(\rho\|\sigma)$. Furthermore,

$$\text{Tr } Q\sigma = \text{Tr}[\{\rho \geq 2^\gamma \sigma\}\sigma] \leq 2^{-\gamma} \text{Tr } \rho \leq 2^{-\gamma},$$

implying that

$$D_H^\varepsilon(\rho\|\sigma) \geq -\log \text{Tr } Q\sigma \geq \gamma = \overline{D}_s^{1-\varepsilon}(\rho\|\sigma) - \delta.$$

Conversely, assume that $D_H^\varepsilon(\rho\|\sigma) < \infty$ and let $0 \leq Q \leq \mathbb{1}$ be optimal for $D_H^\varepsilon(\rho\|\sigma)$, such that

$$\text{Tr } Q\sigma = 2^{-D_H^\varepsilon(\rho\|\sigma)}. \quad (7)$$

For arbitrary κ we have

$$\begin{aligned} 1 - \varepsilon &\leq \text{Tr } Q\rho \\ &= \text{Tr}[Q(\rho - 2^\kappa \sigma)] + 2^\kappa \text{Tr } Q\sigma \\ &\leq \text{Tr}[\{\rho \geq 2^\kappa \sigma\}(\rho - 2^\kappa \sigma)] + 2^{\kappa - D_H^\varepsilon(\rho\|\sigma)}, \end{aligned} \quad (8)$$

where we used Lemma 3.1 and (7) for the first and second terms in the last inequality. Choosing $\kappa = \overline{D}_s^{1-(\varepsilon+\eta)}(\rho\|\sigma) + \delta$ for an arbitrary $\delta > 0$ implies that

$$\text{Tr}(\rho - 2^\kappa \sigma)_+ \leq 1 - (\varepsilon + \eta). \quad (9)$$

From (8) and (9) we have $1 - \varepsilon \leq 1 - (\varepsilon + \eta) + 2^{\kappa - D_H^\varepsilon(\rho\|\sigma)}$ and hence

$$\kappa = \overline{D}_s^{1-(\varepsilon+\eta)}(\rho\|\sigma) + \delta \geq D_H^\varepsilon(\rho\|\sigma) + \log \eta,$$

which results in the lower bound, since δ is arbitrary.

(iii) To prove the lower bound, we set $\gamma = \overline{D}_s^\varepsilon(\rho\|\sigma) + \delta$ for some arbitrary $\delta > 0$. Then we obtain the bounds

$$(\rho - 2^\gamma \sigma)_+ \geq \rho - 2^\gamma \sigma \quad \text{and} \quad \sqrt{8 \text{Tr}(\rho - 2^\gamma \sigma)_+} \leq \sqrt{8\varepsilon},$$

where the second bound follows from the definition of γ . Hence, we can apply Lemma 14 in [9], which yields

$$D_{\max}^{\sqrt{8\varepsilon}}(\rho\|\sigma) \leq \gamma = \overline{D}_s^\varepsilon(\rho\|\sigma) + \delta$$

and therefore implies the result.

Conversely, let $\tilde{\rho}$ achieve the maximum in the definition of $D_{\max}^\varepsilon(\rho\|\sigma)$, i.e. $P(\rho, \tilde{\rho}) \leq \varepsilon$ and $\tilde{\rho} \leq 2^\gamma \sigma$ with $\gamma = D_{\max}^\varepsilon(\rho\|\sigma) + \delta$ for some arbitrary $\delta > 0$. Note that this implies

$$\text{Tr}(\tilde{\rho} - 2^\gamma \sigma)_+ = 0. \quad (10)$$

We proceed by employing the trace distance $d(\rho, \sigma)$, making use of the fact [45] that the trace distance of two subnormalized states ρ and σ can be expressed as

$$d(\rho, \sigma) = \text{Tr}(\rho - \sigma)_+, \quad (11)$$

which is exactly of the form of the trace quantity in the definition of the information spectrum relative entropies. We compute:

$$\begin{aligned} \text{Tr}(\rho - 2^\gamma \sigma)_+ &\leq \text{Tr}[\{\rho > 2^\gamma \sigma\}(\rho - 2^\gamma \sigma)] \\ &= \text{Tr}[\{\rho > 2^\gamma \sigma\}(\rho - \tilde{\rho} + \tilde{\rho} - 2^\gamma \sigma)] \\ &\leq \text{Tr}[\{\rho > \tilde{\rho}\}(\rho - \tilde{\rho})] + \text{Tr}[\{\tilde{\rho} > 2^\gamma \sigma\}(\tilde{\rho} - 2^\gamma \sigma)] \\ &= d(\rho, \tilde{\rho}) \\ &\leq \varepsilon, \end{aligned}$$

where we used Lemma 3.1 in the second inequality and equations (10), (11) and Lemma 3.5 in the following lines. We infer that γ is feasible for $\overline{D}_s^\varepsilon(\rho||\sigma)$, and hence, we obtain

$$\overline{D}_s^\varepsilon(\rho||\sigma) \leq \gamma = D_{\max}^\varepsilon(\rho||\sigma) + \delta,$$

which yields the claim. \square

4.3 Second order asymptotics of the information spectrum relative entropies

In the last section we established bounds for the information spectrum relative entropies $\underline{D}_s^\varepsilon(\rho||\sigma)$ and $\overline{D}_s^\varepsilon(\rho||\sigma)$ in terms of the hypothesis relative testing entropy $D_H^\varepsilon(\rho||\sigma)$. This implies that the second order asymptotic expansion of $D_H^\varepsilon(\rho||\sigma)$ readily carries over to $\underline{D}_s^\varepsilon(\rho||\sigma)$ and $\overline{D}_s^\varepsilon(\rho||\sigma)$. Before we prove this result, for the sake of completeness we briefly outline the procedure used by Tomamichel and Hayashi [47] to obtain the second order asymptotic expansion of $D_H^\varepsilon(\rho||\sigma)$:

For a given state ρ and a positive operator σ with spectral decompositions

$$\rho = \sum_x r_x |v_x\rangle\langle v_x| \quad \text{and} \quad \sigma = \sum_y s_y |u_y\rangle\langle u_y|,$$

consider first the Nussbaum-Szkoła probability distributions defined by

$$P_{\rho,\sigma}(x, y) := r_x |\langle v_x | u_y \rangle|^2 \quad \text{and} \quad Q_{\rho,\sigma}(x, y) := s_y |\langle v_x | u_y \rangle|^2.$$

The usefulness of these distributions lies in the following fact: the first two moments of the log likelihood ratio of $P_{\rho,\sigma}$ and $Q_{\rho,\sigma}$, i.e. the random variable $Z = \log P_{\rho,\sigma}(X, Y) - \log Q_{\rho,\sigma}(X, Y)$ distributed according to the distribution $P_{\rho,\sigma}(x, y)$, agree with the quantum relative entropy and the quantum information variance (given in Definition 3.6), that is,

$$D(P_{\rho,\sigma}||Q_{\rho,\sigma}) = D(\rho||\sigma) \quad \text{and} \quad V(P_{\rho,\sigma}||Q_{\rho,\sigma}) = V(\rho||\sigma). \quad (12)$$

Furthermore, for i.i.d. states $\rho^n \equiv \rho^{\otimes n}$ and $\sigma^n \equiv \sigma^{\otimes n}$ the Nussbaum-Szkoła distributions take on the product form $P_{\rho^n, \sigma^n} = P_{\rho, \sigma}^n$ and $Q_{\rho^n, \sigma^n} = Q_{\rho, \sigma}^n$.

Consider the classical entropic quantity

$$D_s^\varepsilon(P||Q) := \sup\{R \mid \mathbb{P}(\log P - \log Q \leq R) \leq \varepsilon\}.$$

It can be recognized to be the inverse of the cumulative distribution function of the log likelihood ratio Z . The Berry-Esseen theorem [13] states that the random variable $Y = \sqrt{n} \frac{Z - \mu}{s}$ converges to the standard normal distribution and provides a bound on the rate of this convergence. Here,

μ and s are the mean and standard deviation of Z respectively. Carrying over the Berry-Esseen bound to the inverse cumulative distribution functions of Y and Z , we obtain an asymptotic expansion for the quantity $D_s^\varepsilon(P^n\|Q^n)$ in the form of

$$D_s^\varepsilon(P^n\|Q^n) = n\mu + \sqrt{n}s\Phi^{-1}(\varepsilon) + \mathcal{O}(1), \quad (13)$$

where $\Phi^{-1}(\varepsilon)$ is the inverse of the cdf of the standard normal distribution. Choosing $P = P_{\rho,\sigma}$ and $Q = Q_{\rho,\sigma}$ in (13) now connects this asymptotic expansion to ρ and σ , since we have $\mu = D(\rho\|\sigma)$ and $s^2 = V(\rho\|\sigma)$ for $Z = \log P_{\rho,\sigma} - \log Q_{\rho,\sigma}$ according to (12).

The last step consists in finding upper and lower bounds for the relative entropy in question in terms of $D_s^\varepsilon(P_{\rho,\sigma}^n\|Q_{\rho,\sigma}^n)$, which then yields the asymptotic expansion of the former, stated precisely in the following proposition proved in [47].

Proposition 4.8. *Given the i.i.d. states $\rho^{\otimes n}$ and $\sigma^{\otimes n}$, the hypothesis testing relative entropy $D_H^\varepsilon(\rho\|\sigma)$ has the following second order asymptotic expansion:*

$$D_H^\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) = nD(\rho\|\sigma) + \sqrt{n}\mathfrak{s}(\rho\|\sigma)\Phi^{-1}(\varepsilon) + \mathcal{O}(\log n),$$

where $\mathfrak{s}(\rho\|\sigma)$ is defined as in (3) and $\Phi^{-1}(\varepsilon) := \sup\{z \in \mathbb{R} \mid \Phi(z) \leq \varepsilon\}$ is the inverse of the cumulative normal distribution Φ .

This yields the second order asymptotics of the information spectrum relative entropies:

Proposition 4.9. *Given i.i.d. states $\rho^{\otimes n}$ and $\sigma^{\otimes n}$, the second order asymptotic expansions of $\underline{D}_s^\varepsilon(\rho\|\sigma)$ and $\overline{D}_s^\varepsilon(\rho\|\sigma)$ are given by:*

$$(i) \quad \underline{D}_s^\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) = nD(\rho\|\sigma) + \sqrt{n}\mathfrak{s}(\rho\|\sigma)\Phi^{-1}(\varepsilon) + \mathcal{O}(\log n)$$

$$(ii) \quad \overline{D}_s^\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) = nD(\rho\|\sigma) - \sqrt{n}\mathfrak{s}(\rho\|\sigma)\Phi^{-1}(\varepsilon) + \mathcal{O}(\log n)$$

where $\mathfrak{s}(\rho\|\sigma)$ is defined as in (3) and $\Phi^{-1}(\varepsilon) := \sup\{z \in \mathbb{R} \mid \Phi(z) \leq \varepsilon\}$ is the inverse of the cdf of the standard normal distribution.

Proof. We abbreviate $\rho^n \equiv \rho^{\otimes n}$ and $\sigma^n \equiv \sigma^{\otimes n}$.

(i) By Proposition 4.7, (i) we have the following bounds on $\underline{D}_s^\varepsilon(\rho^n\|\sigma^n)$ for any $\delta > 0$:

$$D_H^{\varepsilon-\delta}(\rho^n\|\sigma^n) + \log \delta \leq \underline{D}_s^\varepsilon(\rho^n\|\sigma^n) \leq D_H^\varepsilon(\rho^n\|\sigma^n) \quad (14)$$

Setting $\delta = \frac{1}{\sqrt{n}}$ and applying Proposition 4.8 to the lower bound yields

$$\begin{aligned} D_H^{\varepsilon-\delta}(\rho^n\|\sigma^n) + \log \delta &= D_H^{\varepsilon-\frac{1}{\sqrt{n}}}(\rho^n\|\sigma^n) - \frac{1}{2} \log n \\ &= nD(\rho\|\sigma) + \sqrt{n}\mathfrak{s}(\rho\|\sigma)\Phi^{-1}\left(\varepsilon - \frac{1}{\sqrt{n}}\right) + \mathcal{O}(\log n). \end{aligned} \quad (15)$$

Lemma 3.7 applied to the second term yields

$$\sqrt{n}\Phi^{-1}\left(\varepsilon - \frac{1}{\sqrt{n}}\right) = \sqrt{n}\Phi^{-1}(\varepsilon) + \mathcal{O}(\log n),$$

and substituting this in (15) results in

$$D_H^{\varepsilon-\delta}(\rho^n\|\sigma^n) + \log \delta = nD(\rho\|\sigma) + \sqrt{n}\mathfrak{s}(\rho\|\sigma)\Phi^{-1}(\varepsilon) + \mathcal{O}(\log n).$$

Using the above in the lower bound of (14) and Proposition 4.8 for the upper bound in (14) finally proves the claim.

(ii) Proposition 4.7, (ii) yields the following bounds on $\overline{D}_s^\varepsilon(\rho^n\|\sigma^n)$ for any $\delta > 0$:

$$D_H^{1-\varepsilon-\eta}(\rho^n\|\sigma^n) + \log \eta \leq \overline{D}_s^\varepsilon(\rho^n\|\sigma^n) \leq D_H^{1-\varepsilon}(\rho^n\|\sigma^n) + \delta \quad (16)$$

Setting $\eta = \frac{1}{\sqrt{n}}$, we use Proposition 4.8 in (16), again applying Lemma 3.7 to the lower bound, to obtain

$$\overline{D}_s^\varepsilon(\rho^n\|\sigma^n) = nD(\rho\|\sigma) + \sqrt{n}\mathfrak{s}(\rho\|\sigma)\Phi^{-1}(1-\varepsilon) + \mathcal{O}(\log n).$$

Observing that $\Phi^{-1}(1-\varepsilon) = -\Phi^{-1}(\varepsilon)$ now yields the result. \square

The above results readily imply the asymptotic equipartition property (AEP) for the information spectrum relative entropies:

Proposition 4.10. *Given i.i.d. states $\rho^{\otimes n}$ and $\sigma^{\otimes n}$, then for any $\varepsilon \in (0, 1)$ we have*

$$\lim_{n \rightarrow \infty} \frac{1}{n} \underline{D}_s^\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}) = D(\rho\|\sigma) = \lim_{n \rightarrow \infty} \frac{1}{n} \overline{D}_s^\varepsilon(\rho^{\otimes n}\|\sigma^{\otimes n}).$$

4.4 Relation to the information spectrum method

In the description of information-processing tasks, one usually assumes identical and independently distributed (i.i.d.) input states $\rho^{\otimes n}$, where ρ is a state, if the given protocol is repeated n times. In order to describe more general settings, two different approaches have been proposed. The first one is the smooth entropy framework *one-shot* quantum information theory, initiated by Renner [38, 39, 40] and then considerably extended by himself and others, e.g. Datta [9]. This non-asymptotic approach uses the smooth entropies $D_{\min}^\varepsilon(\rho\|\sigma)$, $D_{\max}^\varepsilon(\rho\|\sigma)$ and $D_H^\varepsilon(\rho\|\sigma)$ to obtain results about information-processing tasks with respect to some error ε . On the other hand, Hayashi et al. [18, 21, 33, 37] adapted the classical information spectrum method, introduced by Han and Verdu [15], to the quantum setting. In [5] the quantum information spectrum method was further developed, and [12] eventually demonstrated that both approaches are equivalent in the sense that the spectral divergences used in the information spectrum method can be obtained as limits of the smooth entropies.

In this section, we derive the analogous results to [12] for the information spectrum relative entropies. Let us first recall the definitions of the spectral divergence rates:

Definition 4.11. Let $\hat{\rho} = \{\rho_n\}_{n \in \mathbb{N}}$ be an arbitrary sequence of states with $\rho_n \in \mathcal{D}(\mathcal{H}^{\otimes n})$ and $\hat{\omega} = \{\omega_n\}_{n \in \mathbb{N}}$ be an arbitrary sequence of positive semi-definite operators with $\omega_n \in \mathcal{P}(\mathcal{H}^{\otimes n})$. Then we define:

(i) the *quantum spectral inf-divergence rate*

$$\underline{D}(\hat{\rho}\|\hat{\omega}) := \sup\{\gamma \mid \liminf_{n \rightarrow \infty} \text{Tr}[\{\rho_n > 2^{n\gamma}\omega_n\}(\rho_n - 2^{n\gamma}\omega_n)] = 1\}. \quad (17)$$

(ii) the *quantum spectral sup-divergence rate*

$$\overline{D}(\hat{\rho}\|\hat{\omega}) := \inf\{\gamma \mid \limsup_{n \rightarrow \infty} \text{Tr}[\{\rho_n > 2^{n\gamma}\omega_n\}(\rho_n - 2^{n\gamma}\omega_n)] = 0\}. \quad (18)$$

\diamond

Remark. Note that the above quantities differ from the spectral divergence rates originally defined in [21]. However, as proved in [5], they are equivalent. \diamond

The quantum spectral divergence rates $\underline{D}(\hat{\rho}\|\hat{\omega})$ and $\overline{D}(\hat{\rho}\|\hat{\omega})$ can be recovered from the information spectrum relative entropies $\underline{D}_s^\varepsilon(\rho\|\sigma)$ and $\overline{D}_s^\varepsilon(\rho\|\sigma)$ respectively in the following way:

Proposition 4.12. *Let $\hat{\rho} = \{\rho_n\}_{n \in \mathbb{N}}$ be an arbitrary sequence of states with $\rho_n \in \mathcal{D}(\mathcal{H}^{\otimes n})$ and let $\hat{\omega} = \{\omega_n\}_{n \in \mathbb{N}}$ be an arbitrary sequence of positive operators with $\omega_n \in \mathcal{P}(\mathcal{H}^{\otimes n})$. Then the following relations hold:*

$$(i) \quad \lim_{\varepsilon \rightarrow 0} \liminf_{n \rightarrow \infty} \frac{1}{n} \underline{D}_s^\varepsilon(\rho_n \| \omega_n) = \underline{D}(\hat{\rho} \| \hat{\omega}) \quad (ii) \quad \lim_{\varepsilon \rightarrow 0} \limsup_{n \rightarrow \infty} \frac{1}{n} \overline{D}_s^\varepsilon(\rho_n \| \omega_n) = \overline{D}(\hat{\rho} \| \hat{\omega})$$

Proof. (i) We first show

$$\lim_{\varepsilon \rightarrow 0} \liminf_{n \rightarrow \infty} \frac{1}{n} \underline{D}_s^\varepsilon(\rho_n \| \omega_n) \leq \underline{D}(\hat{\rho} \| \hat{\omega}). \quad (19)$$

To this end, let $\gamma_n = \underline{D}_s^\varepsilon(\rho_n \| \omega_n)$ and set $c(\varepsilon) := \liminf_{n \rightarrow \infty} \frac{\gamma_n}{n}$. By definition of the limit inferior, for all $\delta > 0$ there exists an N such that $\frac{\gamma_n}{n} > c(\varepsilon) - \delta$ for all $n > N$, or equivalently $\gamma_n > n(c(\varepsilon) - \delta)$. Hence, by definition of $\underline{D}_s^\varepsilon(\rho_n \| \omega_n)$, we have

$$\text{Tr} \left(\rho_n - 2^{n(c(\varepsilon) - \delta)} \omega_n \right)_+ \geq 1 - \varepsilon \quad (20)$$

for all $n > N$. We see that (20) holds for arbitrarily small ε , and hence

$$\liminf_{n \rightarrow \infty} \text{Tr} \left(\rho_n - 2^{n(c(\varepsilon) - \delta)} \omega_n \right)_+ = 1,$$

which implies

$$\underline{D}(\hat{\rho} \| \hat{\omega}) \geq c(\varepsilon) - \delta \quad \text{for all } \varepsilon > 0 \quad (21)$$

by the definition of $\underline{D}(\hat{\rho} \| \hat{\omega})$. Taking the limit $\varepsilon \rightarrow 0$ on both sides of (21) yields

$$\underline{D}(\hat{\rho} \| \hat{\omega}) \geq \lim_{\varepsilon \rightarrow 0} \liminf_{n \rightarrow \infty} \frac{\gamma_n}{n} - \delta,$$

from which we obtain (19).

Conversely, let $\gamma = \underline{D}(\hat{\rho} \| \hat{\omega})$. By the definition of the limit inferior we know that for all $\varepsilon > 0$ there exists an N such that

$$\text{Tr}[\{\rho_n > 2^{n\gamma} \omega_n\}(\rho_n - 2^{n\gamma} \omega_n)] \geq 1 - \varepsilon$$

for all $n > N$. Hence, $n\gamma \leq \underline{D}_s^\varepsilon(\rho_n \| \omega_n)$ for all $n > N$ by the definition of the information spectrum relative entropy, and consequently,

$$\gamma \leq \lim_{\varepsilon \rightarrow 0} \liminf_{n \rightarrow \infty} \frac{1}{n} \underline{D}_s^\varepsilon(\rho_n \| \omega_n),$$

which yields the lower bound in the proposition.

(ii) To prove the upper bound, let $\gamma = \overline{D}(\hat{\rho} \| \hat{\omega})$. By definition of $\overline{D}(\hat{\rho} \| \hat{\omega})$ it holds that

$$\limsup_{n \rightarrow \infty} \text{Tr}(\rho_n - 2^{n\gamma} \omega_n)_+ = 0,$$

that is, for every $\varepsilon > 0$ there exists an N such that

$$\text{Tr}(\rho_n - 2^{n\gamma} \omega_n)_+ < \varepsilon$$

for all $n > N$. By definition of the information spectrum relative entropy, this implies that $\overline{D}_s^\varepsilon(\rho_n \| \omega_n) \leq n\gamma$ for all $n > N$, and hence,

$$\lim_{\varepsilon \rightarrow 0} \limsup_{n \rightarrow \infty} \frac{1}{n} \overline{D}_s^\varepsilon(\rho_n \| \omega_n) \leq \gamma = \overline{D}(\hat{\rho} \| \hat{\omega}).$$

This proves the upper bound.

Conversely, let $\gamma_n = \overline{D}_s^\varepsilon(\rho_n \|\omega_n)$ and set $c(\varepsilon) = \limsup_{n \rightarrow \infty} \frac{\gamma_n}{n}$. By the characterization of the limit superior, for all $\delta > 0$ there exists an N such that $\frac{\gamma_n}{n} < c(\varepsilon) + \delta$ for all $n > N$, or equivalently $\gamma_n < n(c(\varepsilon) + \delta)$. By the definition of γ_n , this implies

$$\text{Tr}(\rho_n - 2^{n(c(\varepsilon) + \delta)} \omega_n)_+ \leq \varepsilon \quad (22)$$

for all $n > N$. Since we take the limit $\varepsilon \rightarrow 0$ and hence ε can be made arbitrarily small in (22), we obtain $\limsup_{n \rightarrow \infty} \text{Tr}(\rho_n - 2^{n(c(\varepsilon) + \delta)} \omega_n)_+ = 0$. Therefore, $\overline{D}(\hat{\rho} \|\hat{\omega}) \leq c(\varepsilon) + \delta$, and taking the limit $\varepsilon \rightarrow 0$ finally yields the result. \square

5 Information-processing tasks: One-shot bounds and second order asymptotics

After having discussed the information spectrum relative entropies and their second order asymptotics in the previous section, we now focus on their application in the following tasks in quantum information theory:

- fixed-length quantum source compression
- noisy dense coding
- entanglement concentration
- pure-state entanglement dilution
- capacity of classical-quantum (cq) channels

For the characteristic quantities in the above tasks, we obtain one-shot bounds in terms of the relative entropies $\underline{D}_s^\varepsilon(\rho \|\sigma)$ and $\overline{D}_s^\varepsilon(\rho \|\sigma)$. Furthermore, using Proposition 4.9 we determine the second order asymptotics of the mentioned tasks, obtaining new results as well as reproducing the second order asymptotics for the capacity of cq-channels from [48].

We employ the following useful lemma due to Hayashi and Nagaoka [21]:

Lemma 5.1. *Let \mathcal{X} denote a finite alphabet and consider a classical-quantum channel $W : \mathcal{X} \mapsto \mathcal{D}(\mathcal{H})$, i.e., $W_x \in \mathcal{D}(\mathcal{H})$ is the output of the channel when the input is $x \in \mathcal{X}$. Then for all $n \in \mathbb{N}$, $\gamma \in \mathbb{R}$, $M \in \mathbb{N}$, a probability distribution $\{p(x)\}_{x \in \mathcal{X}}$ on \mathcal{X} and $c > 0$ there exists a code \mathcal{C} such that $|\mathcal{C}| = M$, and*

$$p_e(\mathcal{C}) \leq (1 + c) \sum_{x \in \mathcal{X}} p(x) \text{Tr} [W_x \{W_x < 2^\gamma \overline{W}\}] + (2 + c + c^{-1}) 2^{-\gamma} M, \quad (23)$$

where $\overline{W} = \sum_{x \in \mathcal{X}} p(x) W_x$.

We also use the following notation:

Definition 5.2. Let $\Theta^{(1),\varepsilon}(\Omega)$ be a quantity characterizing an information-processing task using a resource Ω in the one-shot setting for an error threshold ε . For $n \in \mathbb{N}$, we write

$$\Theta^{n,\varepsilon}(\Omega) := \Theta^{(1),\varepsilon}(\Omega^{\otimes n}).$$

Here, Ω is a placeholder for the resource of the protocol, e.g. a source state $\rho \in \mathcal{D}(\mathcal{H})$ (source coding), a channel Λ , or an entangled pure state $\psi_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ (entanglement conversion). \diamond

5.1 Fixed-length quantum source coding

5.1.1 Blind vs. visible coding

Consider a quantum information source characterized by an ensemble of pure states $\mathfrak{E} = \{p_i, \psi_i\}$ where $|\psi_i\rangle \in \mathcal{H}$ and $\{p_i\}$ being a probability distribution. Note that the pure states ψ_i are not mutually orthogonal in general. Henceforth we shall refer to such an ensemble as the *source ensemble* and the associated density matrix $\rho = \sum_i p_i \psi_i \in \mathcal{D}(\mathcal{H})$ as the *source state*. The pure states ψ_i are the signals emitted by the source with corresponding probabilities p_i .

In fixed-length quantum source coding the aim is to store the information emitted by the source in a *compressed state* $\rho_c \in \mathcal{D}(\mathcal{H}_c)$ with $\dim \mathcal{H}_c < \dim \mathcal{H}$, such that it can be later decompressed to yield a state which is sufficiently close to the source state ρ , with respect to some chosen distance measure. In the one-shot setting, in which one considers a single use of the source, it is natural to allow a non-zero error in the compression-decompression scheme. Hence, a one-shot source-coding protocol is characterized by a parameter ε which denotes the maximum allowed value of the distance between the source state and the state which is obtained after decompression.

There are two different scenarios [17, 1, 51] for the compression part of the protocol outlined above: In the first scenario, which is called the *blind setting*, the encoder (Alice) knows the source state ρ but has no knowledge about the individual signals ψ_i . Hence, in this case the compression map is necessarily a quantum operation $\mathcal{E} : \mathcal{D}(\mathcal{H}) \rightarrow \mathcal{D}(\mathcal{H}_c)$ on the source state. This is called blind source coding.

In contrast, in the second scenario, Alice has complete knowledge about the signals ψ_i as well as their corresponding probabilities p_i . This is the *visible setting*. In fact, Alice essentially has classical information about the pure-state ensemble $\mathfrak{E} = \{p_i, \psi_i\}$ in the form of a list of the probabilities p_i and corresponding pure states ψ_i . She then uses an *arbitrary* map $\mathcal{V} : \{\psi_i\} \rightarrow \mathcal{D}(\mathcal{H}_c)$ to encode the ψ_i in a state $\mathcal{V}(\psi_i) \in \mathcal{D}(\mathcal{H}_c)$ and forming the average ensemble state $\rho_c = \sum_i p_i \mathcal{V}(\psi_i)$. Note that the encoding map \mathcal{V} is not necessarily a quantum operation, since Alice simply prepares a collection of quantum states $\mathcal{V}(\psi_i)$ based on her knowledge of the signal states ψ_i . In particular, \mathcal{V} can be a non-linear map. This is called visible source coding.

In the decompression phase of the protocol, the compressed state $\rho_c = \mathcal{E}(\rho)$ (blind setting) respectively $\rho_c = \sum_i p_i \mathcal{V}(\psi_i)$ (visible setting) is subjected to a quantum operation $\mathfrak{D} : \mathcal{D}(\mathcal{H}_c) \rightarrow \mathcal{D}(\mathcal{H})$.

Interestingly, the optimal rates of both visible and blind source-coding are identical, given by the von Neumann entropy $S(\rho)$ of the ensemble state $\rho = \sum_i p_i \psi_i$ [41, 2, 24]. In the following, we give a complete description of the second order behaviour of visible source-coding and derive bounds on the second order asymptotic expansion in the blind case. In both settings, the optimal rate $S(\rho)$ is retrieved. We derive one-shot bounds on the *minimal compression length*, which is the characteristic quantity of fixed-length quantum source coding and is defined below. These bounds are given in terms of the information spectrum entropy. We then derive second order expansions of these one-shot bounds for sufficiently large n .

5.1.2 One-shot bounds

Let us first define the figures of merit that we use to determine the distance between the input state and the target state of the source-coding protocol:

Definition 5.3.

- (i) For an arbitrary CPTP map $\Lambda : \mathcal{D}(\mathcal{H}) \rightarrow \mathcal{D}(\mathcal{H})$ and a state $\rho \in \mathcal{D}(\mathcal{H})$ with purification

$\psi^\rho \in \mathcal{D}(\mathcal{H} \otimes \mathcal{H}')$, the *entanglement fidelity* $F_e(\rho, \Lambda)$ is defined by

$$F_e(\rho, \Lambda) := \langle \psi^\rho | (\text{id}_{\mathcal{H}'} \otimes \Lambda)(\psi^\rho) | \psi^\rho \rangle.$$

- (ii) Let $\mathfrak{E} = \{p_i, \psi_i\}$ with $\psi_i \in \mathcal{D}(\mathcal{H})$ be a pure-state ensemble and consider an arbitrary map $\mathcal{V} : \{\psi_i\} \rightarrow \mathcal{D}(\mathcal{H}')$ and a CPTP map $\mathfrak{D} : \mathcal{D}(\mathcal{H}') \rightarrow \mathcal{D}(\mathcal{H})$. The *ensemble average fidelity* $\bar{F}(\mathfrak{E}, \mathfrak{D} \circ \mathcal{V})$ is defined by

$$\bar{F}(\mathfrak{E}, \mathfrak{D} \circ \mathcal{V}) := \sum_i p_i \text{Tr}((\mathfrak{D} \circ \mathcal{V})(\psi_i) \psi_i). \quad \diamond$$

We employ the entanglement fidelity and the ensemble average fidelity to define ε -admissible codes in the blind and visible settings respectively. The minimal compression length for a code is then obtained by optimizing over all such codes:

Definition 5.4. Consider a quantum information source with source ensemble $\mathfrak{E} = \{p_i, \psi_i\}$, and source state $\rho = \sum_i p_i \psi_i \in \mathcal{D}(\mathcal{H})$. Let \mathcal{H}_c be a Hilbert space with $M = \dim \mathcal{H}_c < \dim \mathcal{H}$.

- (i) For any $\varepsilon \in (0, 1)$, a visible encoder $\mathcal{V} : \{\psi_i\} \rightarrow \mathcal{D}(\mathcal{H}_c)$ and a CPTP decoder $\mathfrak{D} : \mathcal{D}(\mathcal{H}_c) \rightarrow \mathcal{D}(\mathcal{H})$, the triple $\mathcal{C}_v = (\mathcal{V}, \mathfrak{D}, M)$ is called an ε -admissible (visible) code if

$$\bar{F}(\mathfrak{E}, \mathfrak{D} \circ \mathcal{V}) \geq 1 - \varepsilon.$$

- (ii) For any $\varepsilon \in (0, 1)$, a CPTP encoder $\mathcal{E} : \mathcal{D}(\mathcal{H}) \rightarrow \mathcal{D}(\mathcal{H}_c)$ and a CPTP decoder $\mathfrak{D} : \mathcal{D}(\mathcal{H}_c) \rightarrow \mathcal{D}(\mathcal{H})$, the triple $\mathcal{C}_b = (\mathcal{E}, \mathfrak{D}, M)$ is called an ε -admissible (blind) code if

$$F_e(\rho, \mathfrak{D} \circ \mathcal{E}) \geq 1 - \varepsilon.$$

- (iii) The ε -error one-shot compression length $m_{v/b}^{(1), \varepsilon}(\rho)$ is defined by

$$m_{v/b}^{(1), \varepsilon}(\rho) := \inf\{\log M \mid \exists \text{ an } \varepsilon\text{-admissible code } \mathcal{C}_{v/b} \text{ with } M = \dim \mathcal{H}_c\},$$

where the subscripts v and b are used for the visible and blind setting respectively. \diamond

In the following, we derive one-shot bounds for the minimal compression length.

Theorem 5.5. Consider a quantum information source with source ensemble $\mathfrak{E} = \{p_i, \psi_i\}$, and source state $\rho = \sum_i p_i \psi_i \in \mathcal{D}(\mathcal{H})$. Then for any $\eta > 0$ and $\varepsilon \in (0, 1)$, the ε -error one-shot compression length $m_{v/b}^{(1), \varepsilon}$ satisfies the following bounds:

$$(i) \text{ Visible case: } \overline{H}_s^{\varepsilon+\eta}(\rho) + \log \eta \leq m_v^{(1), \varepsilon}(\rho) \leq \overline{H}_s^\varepsilon(\rho)$$

$$(ii) \text{ Blind case: } \overline{H}_s^{\varepsilon+\eta}(\rho) + \log \eta \leq m_b^{(1), \varepsilon}(\rho) \leq \overline{H}_s^{\varepsilon/2}(\rho)$$

Interestingly, the lower bounds are identical in the two settings. However, the upper bounds are given in terms of the information spectrum entropies with different error parameters. This has consequences on the second order behaviour of $m_b^{(1), \varepsilon}(\rho)$, which we discuss in Section 5.1.5.

5.1.3 Proof of one-shot bounds: Visible setting

Proof of the upper bound in Theorem 5.5(i) (Achievability). Assume that

$$\gamma = \overline{H}_s^\varepsilon(\rho). \quad (24)$$

We set $P = \{\rho \geq 2^{-\gamma} \mathbb{1}\}$ and define the compressed Hilbert space as the image of this projection, i.e. $\mathcal{H}_c := \text{Im } P$. The dimension of \mathcal{H}_c in this case is given by

$$M = \text{Tr } P \leq 2^\gamma, \quad (25)$$

where the inequality follows from Lemma 3.3. Consider now the visible encoding map

$$\mathcal{V} : \psi_i \mapsto \frac{P\psi_i P}{\text{Tr } P\psi_i}.$$

For the decoding map \mathfrak{D} we choose the trivial embedding of the compressed state $\rho_c = \sum_i p_i \mathcal{V}(\psi_i)$ into the original Hilbert space \mathcal{H} . We can verify that this choice of \mathcal{H}_c , \mathcal{V} and \mathfrak{D} constitutes an ε -admissible code \mathcal{C}_v as follows:

$$\begin{aligned} \bar{F}(\mathfrak{E}, \mathfrak{D} \circ \mathcal{V}) &= \sum_i p_i \text{Tr}((\mathfrak{D} \circ \mathcal{V})(\psi_i) \psi_i) \\ &= \sum_i p_i \text{Tr} \frac{P\psi_i P\psi_i}{\text{Tr } P\psi_i} \\ &= \sum_i p_i \frac{\langle \psi_i | P | \psi_i \rangle^2}{\langle \psi_i | P | \psi_i \rangle} \\ &= \sum_i p_i \langle \psi_i | P | \psi_i \rangle \\ &= \text{Tr } P\rho \\ &\geq \text{Tr}[P(\rho - 2^{-\gamma} \mathbb{1})] \\ &\geq 1 - \varepsilon, \end{aligned}$$

where the last inequality follows from the definitions of P and $\overline{H}_s^\varepsilon(\rho)$, and the choice of γ given in (24). Thus, $(\mathcal{V}, \mathfrak{D}, M)$ is an ε -admissible code and we obtain $m_v^{(1),\varepsilon}(\rho) \leq \gamma = \overline{H}_s^\varepsilon(\rho)$ by (25) and Definition 5.4(iii) of the minimal compression length $m_v^{(1),\varepsilon}(\rho)$. \square

In order to prove the lower (converse) bound of Theorem 5.5(i), we employ the following lemma [35, 17]:

Lemma 5.6. *Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ be separable. Then*

$$\begin{aligned} \max\{\text{Tr } P\rho_A \mid P \text{ is a projection on } \mathcal{H}_A \text{ with } \text{Tr } P = k\} \\ \geq \max\{\text{Tr } P\rho_{AB} \mid P \text{ is a projection on } \mathcal{H}_{AB} \text{ with } \text{Tr } P = k\}. \end{aligned}$$

Proof. Since ρ_{AB} is separable, there are states $\sigma_A^{(i)} \in \mathcal{D}(\mathcal{H}_A)$, $\omega_B^{(i)} \in \mathcal{D}(\mathcal{H}_B)$ and a probability distribution $\{\lambda_i\}$ such that $\rho_{AB} = \sum_i \lambda_i \sigma_A^{(i)} \otimes \omega_B^{(i)}$. Since $\omega_B^{(i)} \leq \mathbb{1}_B$ for all i , we have

$$\begin{aligned} \rho_{AB} &= \sum_i \lambda_i \sigma_A^{(i)} \otimes \omega_B^{(i)} \\ &\leq \sum_i \lambda_i \sigma_A^{(i)} \otimes \mathbb{1}_B \\ &= \rho_A \otimes \mathbb{1}_B \end{aligned} \quad (26)$$

where $\rho_A = \sum_i \lambda_i \sigma_A^{(i)}$ is the marginal of ρ_{AB} on \mathcal{H}_A . Let \tilde{P}_{AB} be a maximizing projection in

$$\max\{\text{Tr } P \rho_{AB} \mid P \text{ is a projection on } \mathcal{H}_{AB} \text{ with } \text{Tr } P = k\}$$

and set $\tilde{P}_A = \text{Tr}_B \tilde{P}_{AB}$. Then

$$\text{Tr } \tilde{P}_{AB} \rho_{AB} \leq \text{Tr } \tilde{P}_{AB} (\rho_A \otimes \mathbb{1}_B) = \text{Tr } \tilde{P}_A \rho_A$$

where the inequality follows from (26) and the equality is a property of the partial trace. Since \tilde{P}_A is a projection defined on \mathcal{H}_A with $\text{Tr } \tilde{P}_A = \text{Tr } \tilde{P}_{AB} = k$, the claim follows. \square

The following crucial proposition is due to Hayashi [17]. We reproduce a proof in our notation for the convenience of the reader.

Proposition 5.7. *Consider a quantum information source with source ensemble $\mathfrak{E} = \{p_i, \psi_i\}$, and source state $\rho = \sum_i p_i \psi_i \in \mathcal{D}(\mathcal{H})$. Let $\mathcal{V} : \mathfrak{E} \rightarrow \mathcal{H}_c$ be a visible encoding map into a compressed Hilbert space \mathcal{H}_c , and $\mathfrak{D} : \mathcal{H}_c \rightarrow \mathcal{H}$ be the decompression map. Set $\rho = \sum_i p_i \psi_i$ and denote by $M = \dim \mathcal{H}_c$ the dimension of the compressed Hilbert space \mathcal{H}_c . Then*

$$\bar{F}(\mathfrak{E}, \mathfrak{D} \circ \mathcal{V}) \leq \max\{\text{Tr } P \rho \mid P \text{ is a projection on } \mathcal{H} \text{ with } \text{Tr } P = M\}.$$

Proof. We claim that it suffices to show that

$$\sum_i p_i \text{Tr}(\mathfrak{D}(\chi) \psi_i) \leq \max\{\text{Tr } P \rho \mid P \text{ is a projection on } \mathcal{H} \text{ with } \text{Tr } P = M\} \quad (27)$$

for any pure state $|\chi\rangle \in \mathcal{H}_c$. To see this, consider eigenvalue decompositions $\mathcal{V}(\psi_i) = \sum_j \mu_j^{(i)} \varphi_j^{(i)}$, such that

$$\rho_c = \sum_{i,j} p_i \mu_j^{(i)} \varphi_j^{(i)}.$$

Then our claim follows from linearity of \mathfrak{D} and the trace.

To show (27), let $\mathcal{U} : \mathcal{H}_c \rightarrow \mathcal{H} \otimes \mathcal{H}'$ be a Stinespring isometry of the CPTP map \mathfrak{D} , i.e.

$$\mathfrak{D}(\sigma) = \text{Tr}_{\mathcal{H}'}(\mathcal{U} \sigma \mathcal{U}^\dagger)$$

for $\sigma \in \mathcal{D}(\mathcal{H}_c)$. Then $\mathcal{U} \mathcal{U}^\dagger$ is the projection onto the image of \mathcal{U} in $\mathcal{H} \otimes \mathcal{H}'$. Consider now the pure state

$$\psi'_i := \frac{(\psi_i \otimes \mathbb{1}_{\mathcal{H}'}) \mathcal{U} \chi \mathcal{U}^\dagger (\psi_i \otimes \mathbb{1}_{\mathcal{H}'})}{\text{Tr}(\mathcal{U} \chi \mathcal{U}^\dagger (\psi_i \otimes \mathbb{1}_{\mathcal{H}'}))} \in \mathcal{D}(\mathcal{H} \otimes \mathcal{H}'), \quad (28)$$

which satisfies

$$\begin{aligned} \text{Tr}(\mathcal{U} \chi \mathcal{U}^\dagger) \psi'_i &= \frac{\text{Tr}(\mathcal{U} \chi \mathcal{U}^\dagger (\psi_i \otimes \mathbb{1}_{\mathcal{H}'}) \mathcal{U} \chi \mathcal{U}^\dagger (\psi_i \otimes \mathbb{1}_{\mathcal{H}'}))}{\text{Tr}(\mathcal{U} \chi \mathcal{U}^\dagger (\psi_i \otimes \mathbb{1}_{\mathcal{H}'}))} \\ &= \frac{\langle \chi | \mathcal{U}^\dagger (\psi_i \otimes \mathbb{1}_{\mathcal{H}'}) \mathcal{U} | \chi \rangle^2}{\langle \chi | \mathcal{U}^\dagger (\psi_i \otimes \mathbb{1}_{\mathcal{H}'}) \mathcal{U} | \chi \rangle} \\ &= \langle \chi | \mathcal{U}^\dagger (\psi_i \otimes \mathbb{1}_{\mathcal{H}'}) \mathcal{U} | \chi \rangle \\ &= \text{Tr}(\mathcal{U} \chi \mathcal{U}^\dagger (\psi_i \otimes \mathbb{1}_{\mathcal{H}'})) \\ &= \text{Tr } \mathfrak{D}(\chi) \psi_i. \end{aligned} \quad (29)$$

We claim that

$$\text{Tr}_{\mathcal{H}'} \psi'_i = \psi_i. \quad (30)$$

This can be seen as follows. Firstly, for the denominator of (28) we have

$$\text{Tr}(\mathcal{U}\chi\mathcal{U}^\dagger(\psi_i \otimes \mathbb{1}_{\mathcal{H}'})) = \text{Tr}(\mathfrak{D}(\chi)\psi_i) = \langle \psi_i | \mathfrak{D}(\chi) | \psi_i \rangle. \quad (31)$$

Secondly, the numerator of (28) can be rewritten as

$$\begin{aligned} (\psi_i \otimes \mathbb{1}_{\mathcal{H}'})\mathcal{U}\chi\mathcal{U}^\dagger(\psi_i \otimes \mathbb{1}_{\mathcal{H}'}) &= \left(|\psi_i\rangle\langle\psi_i| \otimes \sum_j |j\rangle\langle j| \right) \mathcal{U}\chi\mathcal{U}^\dagger \left(|\psi_i\rangle\langle\psi_i| \otimes \sum_k |k\rangle\langle k| \right) \\ &= \sum_{j,k} \left[(\langle\psi_i| \otimes \langle j|) \mathcal{U}\chi\mathcal{U}^\dagger (|\psi_i\rangle \otimes |k\rangle) \right] |\psi_i\rangle\langle\psi_i| \otimes |j\rangle\langle k| \end{aligned}$$

where $\{|j\rangle\}$ constitutes an orthonormal basis for \mathcal{H}' . Hence,

$$\begin{aligned} \text{Tr}_{\mathcal{H}'} \left((\psi_i \otimes \mathbb{1}_{\mathcal{H}'}) \mathcal{U}\chi\mathcal{U}^\dagger (\psi_i \otimes \mathbb{1}_{\mathcal{H}'}) \right) &= \text{Tr}_{\mathcal{H}'} \left(\sum_{j,k} \left[(\langle\psi_i| \otimes \langle j|) \mathcal{U}\chi\mathcal{U}^\dagger (|\psi_i\rangle \otimes |k\rangle) \right] \right. \\ &\quad \left. \times |\psi_i\rangle\langle\psi_i| \otimes |j\rangle\langle k| \right) \\ &= \sum_j \left[(\langle\psi_i| \otimes \langle j|) \mathcal{U}\chi\mathcal{U}^\dagger (|\psi_i\rangle \otimes |j\rangle) \right] |\psi_i\rangle\langle\psi_i| \\ &= \langle \psi_i | \mathfrak{D}(\chi) | \psi_i \rangle \psi_i, \end{aligned} \quad (32)$$

where the last equality follows from the definition of the partial trace. Using (31) and (32) in (28) yields (30).

We now want to relate the state ψ'_i to the source state $\rho := \sum_i p_i \psi_i$ associated to \mathfrak{E} . Since ψ'_i is a purification of the pure state ψ_i by (30), there exists a pure state $\phi_i \in \mathcal{D}(\mathcal{H}')$ such that $\psi'_i = \psi_i \otimes \phi_i$. Consequently, the state

$$\rho' := \sum_i p_i \psi'_i = \sum_i p_i \psi_i \otimes \phi_i$$

is separable and satisfies $\text{Tr}_{\mathcal{H}'} \rho' = \rho$. Thus, we can apply Lemma 5.6 to infer that

$$\begin{aligned} \max\{\text{Tr } P\rho' \mid P \text{ is a projection on } \mathcal{H} \otimes \mathcal{H}' \text{ with } \text{Tr } P = M\} \\ \leq \max\{\text{Tr } P\rho \mid P \text{ is a projection on } \mathcal{H} \text{ with } \text{Tr } P = M\}, \end{aligned} \quad (33)$$

and we observe that the projector $\mathcal{U}\mathcal{U}^\dagger$ with

$$\text{Tr } \mathcal{U}\mathcal{U}^\dagger = \text{Tr } \mathcal{U}^\dagger \mathcal{U} = \text{Tr } \mathbb{1}_{\mathcal{H}_c} = M$$

is feasible for the left-hand side of (33). Noting that

$$\chi \leq \mathbb{1}_{\mathcal{H}_c} \quad \text{and thus} \quad \mathcal{U}\chi\mathcal{U}^\dagger \leq \mathcal{U}\mathcal{U}^\dagger, \quad (34)$$

we finally arrive at

$$\begin{aligned} \sum_i p_i \text{Tr}(\mathfrak{D}(\chi)\psi_i) &= \sum_i p_i \text{Tr}((\mathcal{U}\chi\mathcal{U}^\dagger)\psi'_i) \\ &\leq \sum_i p_i \text{Tr}(\mathcal{U}\mathcal{U}^\dagger\psi'_i) \\ &= \text{Tr}(\mathcal{U}\mathcal{U}^\dagger\rho') \\ &\leq \max\{\text{Tr } P\rho' \mid P \text{ is a projection on } \mathcal{H} \otimes \mathcal{H}' \text{ with } \text{Tr } P = M\} \\ &\leq \max\{\text{Tr } P\rho \mid P \text{ is a projection on } \mathcal{H} \text{ with } \text{Tr } P = M\} \end{aligned}$$

where the first line follows from (29), the second line uses (34) and the last line is obtained by applying (33). \square

Proof of the lower bound in Theorem 5.5(i) (Converse). Let $\mathcal{V} : \{\psi_i\} \rightarrow \mathcal{H}_c$ be a visible encoding of the source ensemble \mathfrak{E} into the compressed Hilbert space \mathcal{H}_c with $\dim \mathcal{H}_c = M$, and let $\mathfrak{D} : \mathcal{H}_c \rightarrow \mathcal{H}$ be an arbitrary CPTP map used in the decoding operation. Assuming that

$$\bar{F}(\mathfrak{E}, \mathfrak{D} \circ \mathcal{V}) \geq 1 - \varepsilon,$$

we have to show that

$$\log M \geq \bar{H}_s^{\varepsilon+\eta}(\rho) + \log \eta.$$

To this end, we compute:

$$\begin{aligned} 1 - \varepsilon &\leq \bar{F}(\mathfrak{E}, \mathfrak{D} \circ \mathcal{V}) \\ &\leq \max\{\text{Tr } P\rho \mid P \text{ is a projection on } \mathcal{H} \text{ with } \text{Tr } P = M\} \\ &= \text{Tr } Q\rho \\ &= \text{Tr } Q(\rho - 2^{-\log M + \log \eta} \mathbb{1}) + 2^{-\log M + \log \eta} \text{Tr } Q \\ &\leq \text{Tr}(\rho - 2^{-\log M + \log \eta} \mathbb{1})_+ + \eta \end{aligned}$$

where the second inequality follows from Proposition 5.7, with the maximizing projection denoted by Q satisfying $\text{Tr } Q = M$, and the last inequality uses Lemma 3.1. We have thus shown that, for arbitrary $\eta > 0$

$$1 - (\varepsilon + \eta) \leq \text{Tr}(\rho - 2^{-\log M + \log \eta} \mathbb{1})_+,$$

and hence $\bar{H}_s^{\varepsilon+\eta}(\rho) \leq \log M - \log \eta$, which proves the claim. \square

5.1.4 Proof of one-shot bounds: Blind setting

Proof of the upper bound in Theorem 5.5(ii) (Achievability). Assume that

$$\gamma = \bar{H}_s^{\varepsilon}(\rho). \tag{35}$$

We set $P = \{\rho \geq 2^{-\gamma} \mathbb{1}\}$ and consider the compression map

$$\mathcal{E} : \rho \mapsto P\rho P + \text{Tr}[\rho(\mathbb{1} - P)]|\varphi\rangle\langle\varphi|, \tag{36}$$

where $|\varphi\rangle$ is an arbitrary pure state in the compressed Hilbert space $\tilde{\mathcal{H}}_c \equiv \text{Im } P$ with dimension

$$M = \text{Tr } P \leq 2^\gamma.$$

Here, the inequality follows from Lemma 3.3. For the decoding map \mathfrak{D} we consider the trivial embedding of the compressed state $\mathcal{E}(\rho)$ into the original Hilbert space \mathcal{H}_A . It is known [42] that for a CPTP map Λ with Kraus operators $\{A_i\}$ the entanglement fidelity is given by the expression

$$F_e(\rho, \Lambda) = \sum_i |\text{Tr } A_i \rho|^2.$$

The Kraus form of the compression map \mathcal{E} as in (36) is given by

$$\mathcal{E}(\rho) = P\rho P + \sum_i A_i \rho A_i^\dagger,$$

where $A_i = |\phi\rangle\langle i|$ and $\{|i\rangle\}$ is an orthonormal basis for $(\text{Im } P)^\perp$. We therefore have

$$\begin{aligned} F_e(\rho, \Lambda) &= |\text{Tr } P\rho|^2 + \sum_i |\text{Tr}(|0\rangle\langle i|\rho)|^2 \\ &\geq (\text{Tr } P\rho)^2 \\ &\geq (\text{Tr}[P(\rho - 2^{-\gamma}\mathbf{1})])^2 \\ &= (1 - \varepsilon)^2 \\ &\geq 1 - 2\varepsilon, \end{aligned}$$

where the last equality follows from the definitions of P and $\overline{H}_s^\varepsilon(\rho)$, and the choice of γ given in (35). Thus, $(\mathcal{E}, \mathfrak{D}, M)$ is an 2ε -admissible code, and by replacing ε with $\frac{\varepsilon}{2}$ we obtain $m_b^{(1),\varepsilon}(\rho) \leq \gamma = \overline{H}_s^{\varepsilon/2}(\rho)$ by Definition 5.4(iii) of the compression length $m_b^{(1),\varepsilon}$. \square

For the proof of the lower bound (converse) in Theorem 5.5(ii), we employ the Kraus representation of the CPTP encoding map \mathcal{E} as follows:

Proof of the lower bound in Theorem 5.5(ii) (Converse). We need to prove that for every ε -admissible (blind) coding scheme $\mathcal{C}_b = (\mathcal{E}, \mathfrak{D}, M)$ with $F_e(\rho, \mathfrak{D} \circ \mathcal{E}) \geq 1 - \varepsilon$, the code size M satisfies

$$\log M \geq \overline{H}_s^{\varepsilon+\eta}(\rho) + \log \eta.$$

To this end, let $\mathcal{H}_c \subset \mathcal{H}$ be the compressed Hilbert space with dimension $M = \dim \mathcal{H}_c$, let $\mathcal{E} : \mathcal{D}(\mathcal{H}) \rightarrow \mathcal{D}(\mathcal{H}_c)$ be a CPTP map, and let P be the projector onto \mathcal{H}_c , i.e. $\text{Tr } P = M$. Furthermore, let $\mathfrak{D} : \mathcal{D}(\mathcal{H}_c) \rightarrow \mathcal{D}(\mathcal{H})$ be an arbitrary CPTP map. If $\{E_j\}$ and $\{D_k\}$ are sets of Kraus operators for \mathcal{E} and \mathfrak{D} respectively, then $\{D_k E_j\}$ is a set of Kraus operators for the map $\Lambda = \mathfrak{D} \circ \mathcal{E}$. We also define Q_k as the projector onto the image of D_k , i.e. $Q_k = \Pi_{\text{Im}(D_k P)}$, and note that

$$D_k E_j = Q_k D_k E_j. \quad (37)$$

For all k we have

$$\text{Tr } Q_k = \dim \text{Im}(D_k P) = \dim \text{Im } D_k|_{\text{Im } P} \leq \dim \text{Dom } D_k|_{\text{Im } P} = \dim \text{Im } P = \text{Tr } P. \quad (38)$$

Let us first derive an upper bound for the entanglement fidelity:

$$\begin{aligned} F_e(\rho, \Lambda) &= \sum_{j,k} |\text{Tr}(D_k E_j \rho)|^2 \\ &= \sum_{j,k} |\text{Tr}(Q_k D_k E_j \rho)|^2 \\ &= \sum_{j,k} |\text{Tr}(\sqrt{\rho} Q_k D_k E_j \sqrt{\rho})|^2 \\ &\leq \sum_{j,k} \text{Tr}(Q_k \rho Q_k) \text{Tr}(\sqrt{\rho} E_j^\dagger D_k^\dagger D_k E_j \sqrt{\rho}) \\ &= \sum_{j,k} \text{Tr}(Q_k \rho Q_k) \text{Tr}(D_k E_j \rho E_j^\dagger D_k^\dagger) \end{aligned}$$

where we used (37) in the second equality and the Cauchy-Schwarz inequality for the Hilbert-Schmidt inner product to obtain the inequality. Now let $\tilde{Q} = \arg \max_{Q_k} \text{Tr}(Q_k \rho Q_k)$ and $\eta > 0$

arbitrary, then we can further bound the entanglement fidelity by

$$\begin{aligned}
F_e(\rho, \Lambda) &\leq \text{Tr}(\tilde{Q}\rho\tilde{Q}) \sum_{j,k} \text{Tr}(D_k E_j \rho E_j^\dagger D_k^\dagger) \\
&= \text{Tr} \tilde{Q}\rho \underbrace{\text{Tr} \left(\sum_k D_k \left(\sum_j E_j \rho E_j^\dagger \right) D_k^\dagger \right)}_{=\text{Tr}(\Lambda(\rho))=1} \\
&= \text{Tr}[\tilde{Q}(\rho - 2^{-\log M + \log \eta} \mathbb{1})] + 2^{-\log M + \log \eta} \text{Tr} \tilde{Q} \\
&\leq \text{Tr}(\rho - 2^{-\log M + \log \eta} \mathbb{1})_+ + 2^{-\log M + \log \eta} \text{Tr} P \\
&= \text{Tr}(\rho - 2^{-\log M + \log \eta} \mathbb{1})_+ + \eta
\end{aligned} \tag{39}$$

where we used Lemma 3.1 and (38) in the second inequality. Hence, (39) together with the assumption $F_e(\rho, \mathfrak{D} \circ \mathcal{E}) \geq 1 - \varepsilon$ imply that

$$1 - (\varepsilon + \eta) \leq \text{Tr}(\rho - 2^{-\log M + \log \eta} \mathbb{1})_+.$$

By definition of the information spectrum entropy, we infer that $\overline{H}_s^{\varepsilon+\eta} \leq \log M - \log \eta$. \square

5.1.5 Second order asymptotics of source coding

The one-shot bounds for the optimal source compression length in terms of the information spectrum entropy in Theorem 5.5 together with the asymptotic expansion of the latter in Proposition 4.9 readily yield the second order asymptotic expansion of the visible coding compression length $m_v^{n,\varepsilon}(\rho)$, which is related to the one-shot compression length via Definition 5.2. In the blind setting, Proposition 4.9 provides second order asymptotic bounds for $m_b^{n,\varepsilon}(\rho)$.

Theorem 5.8. *Consider a memoryless quantum source characterized by the pure-state ensemble $\mathfrak{E} = \{p_i, \psi_i\}$ with $\psi_i \in \mathcal{D}(\mathcal{H})$ and the associated average ensemble state $\rho = \sum_i p_i \psi_i$. For any $\varepsilon \in (0, 1)$, the following holds for $m_{v/b}^{n,\varepsilon}(\rho)$:*

(i) *In the visible setting, the second order asymptotic expansion of $m_v^{n,\varepsilon}(\rho)$ is given by*

$$m_v^{n,\varepsilon}(\rho) = nS(\rho) - \sqrt{n(\text{Tr}[\rho(\log \rho)^2] - S(\rho)^2)} \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n). \tag{40}$$

(ii) *In the blind setting, we obtain the following asymptotic bounds:*

$$\begin{aligned}
m_b^{n,\varepsilon}(\rho) &\geq nS(\rho) - \sqrt{n(\text{Tr}[\rho(\log \rho)^2] - S(\rho)^2)} \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n) \\
m_b^{n,\varepsilon}(\rho) &\leq nS(\rho) - \sqrt{n(\text{Tr}[\rho(\log \rho)^2] - S(\rho)^2)} \Phi^{-1}\left(\frac{\varepsilon}{2}\right) + \mathcal{O}(\log n).
\end{aligned} \tag{41}$$

Proof. We abbreviate $\rho^n \equiv \rho^{\otimes n}$. By Theorem 5.5(i) we obtain the following bounds for the compression length in the visible setting with block length n :

$$-\underline{D}_s^{\varepsilon+\eta}(\rho^n \| \mathbb{1}_n) + \log \eta \leq m_v^{n,\varepsilon}(\rho) \leq -\underline{D}_s^\varepsilon(\rho^n \| \mathbb{1}_n).$$

Setting $\eta = \frac{1}{\sqrt{n}}$, Proposition 4.9 implies

$$\begin{aligned}
m_v^{n,\varepsilon}(\rho) &\geq -nD(\rho \| \mathbb{1}) - \sqrt{n} \mathfrak{s}(\rho \| \mathbb{1}) \Phi^{-1}\left(\varepsilon + \frac{1}{\sqrt{n}}\right) + \mathcal{O}(\log n) \\
m_v^{n,\varepsilon}(\rho) &\leq -nD(\rho \| \mathbb{1}) - \sqrt{n} \mathfrak{s}(\rho \| \mathbb{1}) \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n).
\end{aligned}$$

We apply Lemma 3.7 to the lower bound and use $S(\rho) = -D(\rho\|\mathbb{1})$ to obtain

$$m_v^{n,\varepsilon}(\rho) = nS(\rho) - \sqrt{n} \mathfrak{s}(\rho\|\mathbb{1}) \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n).$$

Expanding the term $\mathfrak{s}(\rho\|\mathbb{1})$ gives

$$\begin{aligned} \mathfrak{s}(\rho\|\mathbb{1}) &= \sqrt{\text{Tr}[\rho_A(\log \rho - \log \mathbb{1})^2] - D(\rho\|\mathbb{1})^2} \\ &= \sqrt{\text{Tr}[\rho(\log \rho)^2] - S(\rho)^2}, \end{aligned}$$

which yields the result. The bounds for the blind setting follow analogously. \square

Remark.

- (i) We note that the ‘gap’ in the second order asymptotic bounds (41) for $m_b^{(1),\varepsilon}(\rho)$ is due to the different error parameters ε and $\frac{\varepsilon}{2}$ in Theorem 5.5(ii). Hence, our method only yields non-matching asymptotic bounds in the blind setting. Closing this gap and deriving a closed form of the second order asymptotic expansion as in the visible setting, (40), remains an open question.
- (ii) Using the result in Theorem 5.8, we are able to recover the second order asymptotics of classical fixed-length source coding derived by Hayashi (see Theorems 3 and 9 of [19]).
- (iii) Note that $\Phi^{-1}(\varepsilon) > 0$ for $\varepsilon > \frac{1}{2}$, and therefore, the second order term in (40) is strictly negative. In this case, the compression rate to second order drops below the von Neumann entropy $S(\rho)$, as illustrated in Figure 2, since the former is given by $\frac{an+b\sqrt{n}}{n}$ where $a = S(\rho)$ and $b = -\sqrt{(\text{Tr}[\rho(\log \rho)^2] - S(\rho)^2)} \Phi^{-1}(\varepsilon)$.

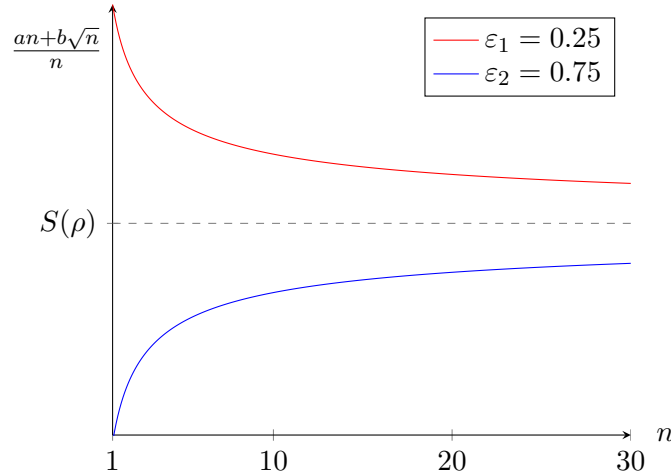


Figure 2: Plot of $\frac{an+b\sqrt{n}}{n}$ for the source state $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +|$.

5.2 Noisy dense coding

Dense coding is the protocol by which prior shared entanglement between a sender (Alice) and a receiver (Bob) is exploited for sending classical messages through a noiseless quantum channel. If the entanglement shared between Alice and Bob is in the form of a mixed state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ (instead of a maximally entangled pure state), then the entanglement is said to be noisy.

Our aim is to derive second order asymptotics for the optimal rate of reliable transmission of classical information through a noiseless quantum channel, assisted by prior shared noisy entanglement. If the noisy entanglement is in the form of multiple, identical copies of a bipartite state ρ_{AB} , then the optimal rate in the asymptotic limit is referred to as the *dense coding capacity* of the state ρ_{AB} and denoted by $C_{dc}(\rho_{AB})$.

In [25], it was shown that

$$C_{dc}(\rho_{AB}) = \log d + S(\rho_B) - \inf_n \inf_{\Lambda^{(n)}} \frac{1}{n} S((\Lambda^{(n)} \otimes \text{id}_{B^n}) \rho_{AB}^{\otimes n}),$$

where $\Lambda^{(n)}$ is a CPTP map acting on states on $\mathcal{H}_A^{\otimes n}$ and $d = \dim \mathcal{H}_A$. If only product encodings of the form $\Lambda^{\otimes n}$ are allowed, the above expression reduces to

$$C_{dc}(\rho_{AB}) = \log d + S(\rho_B) - \inf_{\Lambda: \text{CPTP}} S((\Lambda \otimes \text{id}_B) \rho_{AB}),$$

which was derived independently by Winter in [52].

In the present work, we restrict ourselves to the latter case. As a first step, we derive upper and lower bounds on the maximum number of bits of a classical message which can be transmitted through a single use of the channel, with a probability of error at most ε , for a given $0 < \varepsilon < 1$. We then discuss the i.i.d. case under the assumption of a product encoding. In the following, we briefly summarize the coding procedure:

Let ρ_{AB} be the noisy entangled state that Alice shares with Bob, the system A being with Alice and B being with Bob. Suppose Alice has a set of classical messages labelled by the elements of the set $\mathcal{M} := \{1, 2, \dots, M\}$, which she wishes to send to Bob through a noiseless quantum channel. The most general protocol for this consists of an encoding map by Alice on her system A , transmission of the encoded state through the noiseless channel to Bob, followed by a decoding operation by Bob on the joint state of the system that he receives and the system B .

The codewords are given by

$$\varphi(m) = (\mathcal{E}_A^m \otimes \text{id}_B) \rho_{AB} = \sigma_{AB}^m, \quad m \in \mathcal{M}.$$

Here, φ denotes the encoding map for a code of size M , as defined in terms of the CPTP maps \mathcal{E}_A^m for $m \in \mathcal{M}$. Since the system A is sent through a noiseless channel, the final state in Bob's possession (when Alice sends the message m) is σ_{AB}^m . Let Bob's decoding map be given by the POVM $Y = \{Y_{AB}^m\}_{m \in \mathcal{M}}$. The triple (φ, Y, M) defines a code \mathcal{C} of size M , with average probability of error given by

$$p_e(\mathcal{C}) := \frac{1}{M} \sum_{m=1}^M (1 - \text{Tr}(\sigma_{AB}^m Y_{AB}^m)).$$

Definition 5.9. For $\varepsilon > 0$, the ε -error one-shot dense coding capacity of the state ρ_{AB} is defined as

$$C_{dc}^{(1),\varepsilon}(\rho_{AB}) := \sup\{\log M \mid \exists \text{ a code } \mathcal{C} = (\varphi, Y, M) \text{ such that } p_e(\mathcal{C}) \leq \varepsilon\}. \quad \diamond$$

5.2.1 One-shot bounds for noisy dense coding

We obtain the following bounds on the ε -error one-shot dense coding capacity of a bipartite state ρ_{AB} :

Theorem 5.10. Fix $\varepsilon > 0$. Let $c, \eta, \eta' > 0$ with $\eta > \frac{c}{1+c}\varepsilon$ and $\delta > 0$. The one-shot ε -error dense coding capacity of a state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ satisfies the following bounds:

$$\begin{aligned} C_{dc}^{(1),\varepsilon}(\rho_{AB}) &\geq \log d_A - \min_{\Lambda^{A \rightarrow A}} \overline{H}_s^{\varepsilon-\eta}(A|B)_\sigma + \log \frac{c}{1+c} + \log \left(\eta - \frac{c}{1+c}\varepsilon \right) \\ C_{dc}^{(1),\varepsilon}(\rho_{AB}) &\leq \log d_A - \min_{\Lambda^{A \rightarrow A}} \overline{H}_s^{\varepsilon+\eta'}(A|B)_\sigma + \delta - \log \eta', \end{aligned}$$

where $d_A = \dim \mathcal{H}_A$ and $\sigma_{AB} := (\Lambda \otimes \text{id}_B)\rho_{AB}$ for any CPTP map $\Lambda^{A \rightarrow A}$.

Proof of the upper bound in Theorem 5.10 (Converse). To establish the converse bound, it suffices to prove that for any code \mathcal{C} of M codewords with

$$\log M > \log d_A - \min_{\Lambda^{A \rightarrow A}} \overline{H}_s^\varepsilon(A|B)_\sigma + \delta - \log \eta', \quad (42)$$

where $d_A = \dim \mathcal{H}_A$, and $\sigma_{AB} := (\Lambda \otimes \text{id}_B)\rho_{AB}$ for any CPTP map $\Lambda^{A \rightarrow A}$, we must have $p_e(\mathcal{C}) > \varepsilon$.

If a code \mathcal{C} of size M has codewords $\sigma_{AB}^m = (\mathcal{E}_A^m \otimes \text{id}_B)\rho_{AB}$, and measurement operators Y_{AB}^m for $m \in \mathcal{M}$, then for any $\gamma > 0$ we have

$$\begin{aligned} p_e(\mathcal{C}) &= 1 - \frac{1}{M} \sum_{m=1}^M \text{Tr} [Y_{AB}^m (\sigma_{AB}^m - 2^{-\gamma}(\mathbb{1}_A \otimes \rho_B))] - \frac{2^{-\gamma}}{M} \sum_{m=1}^M \text{Tr} [Y_{AB}^m (\mathbb{1}_A \otimes \rho_B)] \\ &\geq 1 - \frac{1}{M} \sum_{m=1}^M \text{Tr} [\{\sigma_{AB}^m \geq 2^{-\gamma} \mathbb{1}_A \otimes \rho_B\} (\sigma_{AB}^m - 2^{-\gamma} \mathbb{1}_A \otimes \rho_B)] - \frac{2^{-\gamma}}{M} \text{Tr} \mathbb{1}_A \\ &\geq 1 - \max_{m \in \mathcal{M}} \text{Tr} [\{\sigma_{AB}^m \geq 2^{-\gamma} \mathbb{1}_A \otimes \rho_B\} (\sigma_{AB}^m - 2^{-\gamma} \mathbb{1}_A \otimes \rho_B)] - \frac{2^{\log d_A - \gamma}}{M}, \end{aligned} \quad (43)$$

where we used Lemma 3.1 and the fact that $\sum_{m \in \mathcal{M}} Y_{AB}^m = \mathbb{1}_{AB}$ in the first inequality and $\text{Tr} \mathbb{1}_A = d_A$ in the second inequality.

For some arbitrary $\eta', \delta > 0$, choose

$$\begin{aligned} \gamma &= \min_{\Lambda^{A \rightarrow A}} \overline{H}_s^{\varepsilon+\eta'}(A|B)_\sigma - \delta \leq \overline{H}_s^{\varepsilon+\eta'}(A|B)_{\sigma_m} - \delta \\ &\leq \overline{H}_s^{\varepsilon+\eta'}(A|B)_{\sigma_m} - \delta \end{aligned} \quad (44)$$

where $\sigma_{AB} := (\Lambda \otimes \text{id}_B)\rho_{AB}$ and σ_{AB}^m is any codeword. The inequality holds because $\sigma_{AB}^m = (\mathcal{E}_A^m \otimes \text{id}_B)\rho_{AB}$ with $\mathcal{E}_A^m \otimes \text{id}_B$ being a CPTP map, and hence

$$\overline{H}_s^{\varepsilon+\eta'}(A|B)_{\sigma_m} \geq \min_{\Lambda^{A \rightarrow A}} \overline{H}_s^{\varepsilon+\eta'}(A|B)_\sigma.$$

The choice of γ in (44) yields

$$\text{Tr} [\{\sigma_{AB}^m \geq 2^{-\gamma} \mathbb{1}_A \otimes \rho_B\} (\sigma_{AB}^m - 2^{-\gamma} \mathbb{1}_A \otimes \rho_B)] < 1 - (\varepsilon + \eta'), \quad (45)$$

and by (42), (43) and (45), we obtain

$$\begin{aligned} p_e(\mathcal{C}) &> \varepsilon + \eta' - 2^{\log d - \gamma - \log M} \\ &> \varepsilon + \eta' - 2^{\log \eta'} \\ &= \varepsilon. \end{aligned} \quad \square$$

Proof of the lower bound in Theorem 5.10 (Achievability). To establish the lower bound, we use Lemma 5.1. For our purpose, we define $\mathcal{X} := \{(p, q) \mid 0 \leq p, q \leq d_A - 1\}$ (such that $|\mathcal{X}| = d_A^2$) and consider the classical-quantum (c-q) channel

$$W : x \in \mathcal{X} \mapsto W_x \equiv W_{AB}^x := (\mathcal{U}_x \otimes \text{id}_B) \sigma_{AB}. \quad (46)$$

Here, $\sigma_{AB} := (\Lambda \otimes \text{id}_B) \rho_{AB}$ where $\Lambda^{A \rightarrow A}$ denotes the minimizing CPTP map in

$$\min_{\Lambda^{A \rightarrow A}} \overline{H}_s^{\varepsilon+\eta}(A|B)_\sigma,$$

and ρ_{AB} is the initial entangled state shared between Alice and Bob. For $x = (p, q) \in \mathcal{X}$, the unitary encoding \mathcal{U}_x is defined by $\mathcal{U}_x(\rho) := U_{p,q} \rho U_{p,q}^\dagger$. The Weyl operators [23] $U_{p,q}$ with $p, q \in \{0, 1, \dots, (d_A - 1)\}$ are defined by $U_{p,q} = X^q Z^p$ where for any orthonormal basis $\{|j\rangle : j \in \{0, 1, \dots, (d - 1)\}\}$ in a d -dimensional Hilbert space \mathcal{H} the action of X and Z is given by $X|j\rangle = |(j+1) \bmod d\rangle$ and $Z|j\rangle = e^{\frac{2\pi i j}{d}}|j\rangle$. Hence,

$$U_{p,q} = e^{\frac{2\pi i p j}{d}} |(j+q) \bmod d\rangle.$$

Furthermore, it is known that

$$\sum_{x \in \mathcal{X}} \mathcal{U}_x(\omega) \equiv \sum_{p,q} U_{p,q} \omega U_{p,q}^\dagger = d \mathbb{1} \quad (47)$$

for any $\omega \in \mathcal{D}(\mathcal{H})$, with $d = \dim(\mathcal{H})$.

Now let $\{p(x)\}_{x \in \mathcal{X}}$ denote the uniform distribution on \mathcal{X} , i.e. $p(x) = 1/d_A^2$ for all $x \in \mathcal{X}$. For the ensemble $\{p(x), W_{AB}^x\}$, where the states W_{AB}^x are defined by (46), we have by (47) that

$$\begin{aligned} \overline{W}_{AB} &:= \sum_{x \in \mathcal{X}} p(x) W_{AB}^x = \frac{1}{d_A^2} \sum_{x \in \mathcal{X}} (\mathcal{U}_x \otimes \text{id}_B) \sigma_{AB} \\ &= \frac{\mathbb{1}_A}{d_A} \otimes \rho_B, \end{aligned}$$

with $\rho_B = \sigma_B = \text{Tr}_A \sigma_{AB}$. Setting $\alpha := \sum_{x \in \mathcal{X}} p(x) \text{Tr} [W_{AB}^x \{W_{AB}^x \geq 2^\gamma \overline{W}_{AB}\}]$, we obtain

$$\begin{aligned} \alpha &\geq \frac{1}{d_A^2} \sum_{x \in \mathcal{X}} \text{Tr} [\{W_{AB}^x \geq 2^\gamma \overline{W}_{AB}\} (W_{AB}^x - 2^\gamma \overline{W}_{AB})] \\ &= \frac{1}{d_A^2} \sum_{x \in \mathcal{X}} \text{Tr} \left[\{W_{AB}^x \geq 2^{-(\log d_A - \gamma)} \mathbb{1}_A \otimes \rho_B\} (W_{AB}^x - 2^{-(\log d_A - \gamma)} \mathbb{1}_A \otimes \rho_B) \right] \\ &= \frac{1}{d_A^2} \sum_{x \in \mathcal{X}} \text{Tr} \left[\{\sigma_{AB} \geq 2^{-(\log d_A - \gamma)} (\mathbb{1}_A \otimes \rho_B)\} (\sigma_{AB} - 2^{-(\log d_A - \gamma)} (\mathbb{1}_A \otimes \rho_B)) \right]. \end{aligned}$$

In the above we have made use of the fact that

$$\begin{aligned} \{W_{AB}^x \geq 2^\gamma \overline{W}_{AB}\} &= \left\{ (\mathcal{U}_x \otimes \text{id}_B) \sigma_{AB} \geq 2^\gamma (\mathcal{U}_x \otimes \text{id}_B) \left(\frac{\mathbb{1}_A}{d_A} \otimes \rho_B \right) \right\} \\ &= \{\sigma_{AB} \geq 2^{-(\log d_A - \gamma)} (\mathbb{1}_A \otimes \rho_B)\}, \end{aligned}$$

and the fact that the trace remains invariant under a unitary transformation.

Choose

$$\gamma = \log d_A - \overline{H}_s^{\varepsilon-\eta}(A|B)_\sigma = \log d_A - \min_{\Lambda^{A \rightarrow A}} \overline{H}_s^{\varepsilon-\eta}(A|B)_\sigma, \quad (48)$$

for some arbitrary $\eta > 0$. The second identity in (48) follows from the fact that σ_{AB} is the minimizing state in (46). For this choice of γ , $\alpha \geq 1 - (\varepsilon - \eta)$. Using this in (23) of Lemma 5.1 we infer that, for the c-q channel W defined by (46), there exists a code \mathcal{C} of size M such that

$$p_e(\mathcal{C}) \leq (1+c)(\varepsilon - \eta) + (2+c+c^{-1})2^{-\gamma}M.$$

Thus, $p_e(\mathcal{C}) \leq \varepsilon$ for the choice

$$(1+c)(\varepsilon - \eta) + (2+c+c^{-1})2^{-\gamma}M = \varepsilon,$$

and hence,

$$\frac{(1+c)^2}{c}2^{-\gamma}M = (1+c)\eta - c\varepsilon.$$

We obtain

$$\begin{aligned} \log M &= \gamma + \log \frac{c}{1+c} + \log \left(\eta - \frac{c}{1+c}\varepsilon \right) \\ &= \log d_A - \min_{\Lambda^{A \rightarrow A}} \overline{H}_s^{\varepsilon-\eta}(A|B)_\sigma + \log \frac{c}{1+c} + \log \left(\eta - \frac{c}{1+c}\varepsilon \right). \end{aligned}$$

Note that the argument of the logarithm in the right-most term yields the condition $\eta > \frac{c}{1+c}\varepsilon$. The above implies that for the dense coding protocol employing the entangled state ρ_{AB} , we have the following bound:

$$C_{dc}^{(1),\varepsilon}(\rho_{AB}) \geq \log d_A - \min_{\Lambda^{A \rightarrow A}} \overline{H}_s^{\varepsilon-\eta}(A|B)_\sigma + \log \frac{c}{1+c} + \log \left(\eta - \frac{c}{1+c}\varepsilon \right)$$

This inference follows from the fact that in the dense coding protocol, after her encoding, Alice can post-process her system A by $\mathcal{U}_x \circ \Lambda$ (where Λ is some CPTP map) before sending it through the noiseless channel to Bob. \square

5.2.2 Second order asymptotics of noisy dense coding

In order to obtain the second order asymptotics of the ε -error one-shot dense coding capacity $C_{dc}^{(1),\varepsilon}$, we restrict our analysis to the case where Alice is only allowed to use product encodings. More precisely, given an initial state ρ_{AB} , Alice chooses an encoding map $\Lambda^{A \rightarrow A}$. Her encoding map on $\rho_{AB}^{\otimes n}$ results in the state $((\Lambda \otimes \text{id}_B)(\rho_{AB}))^{\otimes n}$, which is transmitted to Bob through the noiseless channel. This is in contrast to the general setting, where Alice selects an encoding map $\Lambda^{(n)} : A^n \rightarrow A^n$ for each n and transmits the state $(\Lambda^{(n)} \otimes \text{id}_{B^n})(\rho_{AB}^{\otimes n})$ [25].

Using the results from Section 4.3, we obtain the following second order expansion for $C_{dc}^{n,\varepsilon}(\rho_{AB})$, which is related to the one-shot dense coding capacity via Definition 5.2.

Theorem 5.11. *Consider an arbitrary bipartite state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$. For any $\varepsilon \in (0,1)$, the second order asymptotic expansion of $C_{dc}^{n,\varepsilon}(\rho_{AB})$ is given by*

$$\begin{aligned} C_{dc}^{n,\varepsilon}(\rho_{AB}) &= n \left(\log d_A + S(\rho_B) - \min_{\Lambda^{A \rightarrow A}} S((\Lambda \otimes \text{id})(\rho_{AB})) \right) \\ &\quad + \sqrt{n} \max_{\Lambda^{A \rightarrow A}} s((\Lambda \otimes \text{id})(\rho_{AB})) \|\mathbb{1}_A \otimes \rho_B\| \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n). \end{aligned}$$

Proof. For arbitrary $\delta > 0$ we have the following one-shot bounds by Theorem 5.10:

$$C_{dc}^{n,\varepsilon}(\rho_{AB}) \geq n \log d_A - \min_{\Lambda^{A \rightarrow A}} \overline{H}_s^{\varepsilon-\eta}(A^n|B^n)_{\sigma^n} + \log \frac{c}{1+c} + \log \left(\eta - \frac{c}{1+c} \varepsilon \right) \quad (49)$$

for $\eta > \frac{c}{1+c} \varepsilon$ and

$$C_{dc}^{n,\varepsilon}(\rho_{AB}) \leq n \log d_A - \min_{\Lambda^{A \rightarrow A}} \overline{H}_s^{\varepsilon+\eta'}(A^n|B^n)_{\sigma^n} + \delta - \log \eta' \quad (50)$$

for $\eta' > 0$. In (49) and (50) we set $\sigma^n \equiv \sigma_{AB}^{\otimes n}$ where $\sigma_{AB} := (\Lambda \otimes \text{id}_B)(\rho_{AB})$.

We would like to set $\eta = \eta' = \frac{1}{\sqrt{n}}$ in the above bounds, as in the proof of Proposition 4.9. To this end, let us choose $c = \frac{1}{n}$ for the constant from Lemma 5.1, which then guarantees the existence of a code \mathcal{C}_n of size M_n such that

$$\log M_n = \gamma + \log \left(\frac{1+n}{n} \eta - \frac{1}{n} \varepsilon \right) - \log n + 2 \log(1+n),$$

subject to the condition

$$\eta > \frac{1}{1+n} \varepsilon.$$

This in turn implies a lower bound on the ε -error capacity $C_{dc}(n, \varepsilon)$ given by

$$\begin{aligned} C_{dc}^{n,\varepsilon}(\rho_{AB}) &\geq n \log d_A - \min_{\Lambda^{A \rightarrow A}} \overline{H}_s^{\varepsilon-\eta}(A^n|B^n)_{\sigma^n} \\ &\quad + \log \left(\frac{1+n}{n} \eta - \frac{1}{n} \varepsilon \right) - \log n + 2 \log(1+n). \end{aligned} \quad (51)$$

We observe that for $0 < \varepsilon < 1$ we have

$$\frac{1}{\sqrt{n}} > \frac{1}{1+n} > \frac{1}{1+n} \varepsilon,$$

and thus, the choice $\eta = \frac{1}{\sqrt{n}}$ is valid in (51).

We can therefore choose $\eta = \eta' = \frac{1}{\sqrt{n}}$ and apply Proposition 4.9 to $\overline{H}_s^{\varepsilon \pm \eta}(A^n|B^n)_{\sigma^n}$ in (50) and (51) in the following way:

$$\begin{aligned} -\overline{H}_s^{\varepsilon \pm \eta}(A^n|B^n)_{\sigma^n} &= \underline{D}_s^{\varepsilon \pm \eta}(\sigma_{AB}^n \| \mathbb{1}_{A^n} \otimes \rho_B^n) \\ &= nD(\sigma_{AB} \| \mathbb{1}_A \otimes \rho_B) + \sqrt{n} \mathfrak{s}(\sigma_{AB} \| \mathbb{1}_A \otimes \rho_B) \Phi^{-1}(\varepsilon \pm \eta) + \mathcal{O}(\log n) \\ &= -nS(\sigma_{AB}) + nS(\rho_B) + \sqrt{n} \mathfrak{s}(\sigma_{AB} \| \mathbb{1}_A \otimes \rho_B) \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n) \end{aligned} \quad (52)$$

where the last equality follows from Lemma 3.7 and the fact that $\text{Tr}_A \sigma_{AB} = \rho_B$. Substituting (52) in (50) and (51) yields the result. \square

Theorem 5.11 immediately implies the first order asymptotics of noisy dense coding as in [52]:

Corollary 5.12. *In the asymptotic limit, the noisy dense coding capacity of a bipartite state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ reads*

$$C_{dc}(\rho_{AB}) = \log d_A + S(\rho_B) - \inf_{\Lambda: CPTP} S((\Lambda \otimes \text{id}_B)\rho_{AB}),$$

where $d_A = \dim \mathcal{H}_A$.

5.3 Entanglement concentration

Entanglement concentration is the protocol in which two parties, Alice and Bob, share a partially entangled state $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, and they wish to convert it into a maximally entangled state $|\Phi_M^+\rangle$ (of Schmidt rank M) by local operations and classical communication (LOCC) alone. If Λ denotes the LOCC map used by Alice and Bob, then the fidelity of the protocol is given by

$$F(\Lambda(\psi_{AB}), \Phi_M^+) := \langle \Phi_M^+ | \Lambda(\psi_{AB}) | \Phi_M^+ \rangle.$$

Note that the above definition of fidelity (which is also used in Sections 5.4 and 5.5) is the square of the one defined previously. For given orthonormal bases $\{|\tilde{k}_A\rangle\}_{k=1}^{d_A}$ and $\{|\tilde{k}_B\rangle\}_{k=1}^{d_B}$ in Hilbert spaces \mathcal{H}_A and \mathcal{H}_B of dimensions d_A and d_B respectively, we define the canonical maximally entangled state of Schmidt rank $M = \min\{d_A, d_B\}$ as

$$|\Phi_M^+\rangle = \frac{1}{\sqrt{M}} \sum_{k=1}^M |\tilde{k}_A\rangle |\tilde{k}_B\rangle. \quad (53)$$

In fact, in the following we consider $\mathcal{H}_A \simeq \mathcal{H}_B$, for simplicity, so that $d_A = d_B = d$ (say).

Definition 5.13. For any $\varepsilon > 0$ the one-shot ε -error distillable entanglement of the pure state ψ_{AB} is defined as

$$E_D^{(1),\varepsilon}(\psi_{AB}) := \sup\{\log M \mid \exists \text{ an LOCC map } \Lambda \text{ such that } F(\Lambda(\psi_{AB}), \Phi_M^+) \geq 1 - \varepsilon\}. \quad \diamond$$

Bennett et al. [4] established that in the asymptotic limit requiring perfect concentration (i.e. $\varepsilon \rightarrow 0$) yields the optimal rate of entanglement concentration to be the entropy of entanglement, i.e. the von Neumann entropy $S(\rho_A)$ of the reduced state $\rho_A = \text{Tr}_B \psi_{AB}$:

$$\lim_{\varepsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} E_D^{n,\varepsilon}(\psi_{AB}) = S(\rho_A)$$

In this section we determine the asymptotic behaviour to second order of the ε -error distillable entanglement.

5.3.1 One-shot bounds for entanglement concentration

We obtain the following bounds on the distillable entanglement:

Theorem 5.14. Fix $\varepsilon > 0$ and let $\delta, \eta > 0$. Then the one-shot ε -error distillable entanglement of a pure state ψ_{AB} satisfies the bounds

$$\underline{H}_s^{\varepsilon-\eta}(\rho_A) + \log \eta + \log(1 - \varepsilon) - \Delta \leq E_D^{(1),\varepsilon}(\psi_{AB}) \leq -\overline{H}_s^{\varepsilon+\eta}(A|B)_\psi + \delta - \log \eta, \quad (54)$$

where Δ is a number included to ensure that the left-hand side is the logarithm of an integer.

Proof of the lower bound in Theorem 5.14 (Achievability). Let the bipartite state $|\psi_{AB}\rangle$ have the Schmidt decomposition

$$|\psi_{AB}\rangle = \sum_k \sqrt{\lambda_k} |e_k^A\rangle |e_k^B\rangle,$$

and let $\rho_A = \text{Tr}_B \psi_{AB}$ and define projection operators $Q = \{\rho_A < 2^{-\gamma} \mathbb{1}_A\}$ and $\overline{Q} = \mathbb{1}_A - Q$, for some $\gamma > 0$.

The first step of the protocol is for one of the parties (say, Alice) to do a von Neumann measurement, described by the projection operators Q and \overline{Q} , on her part of the shared bipartite

state ψ_{AB} . If the outcome of the measurement corresponds to \overline{Q} , then the protocol is aborted as unsuccessful. This occurs with probability

$$P_{fail} = \text{Tr } \overline{Q} \rho_A.$$

If the outcome of the measurement corresponds to Q , then the post-measurement state is given by

$$|\psi'_{AB}\rangle := \frac{1}{\sqrt{\text{Tr } Q \rho_A}} \sum_{\lambda_k < 2^{-\gamma}} \sqrt{\lambda_k} |e_k^A\rangle |e_k^B\rangle,$$

and each of the eigenvalues of the reduced density matrix of this state is bounded from above by

$$\frac{2^{-\gamma}}{\text{Tr } Q \rho_A}.$$

Nielsen's majorization theorem [34] states that a bipartite pure state Ψ with subsystem state σ may be converted by LOCC into the pure state Φ with subsystem state ω , if and only if the ordered eigenvalues of σ are majorized by those of ω . Specifically,

$$\sum_{m=1}^k \nu_m \leq \sum_{m=1}^k \mu_m \quad (55)$$

for all $1 \leq k \leq d$, with equality holding for $k = d$. Here $\{\nu_m\}$ and $\{\mu_m\}$ denote the sets of eigenvalues of Ψ and Φ respectively, labelled in a manner such that $\nu_1 \geq \nu_2 \geq \dots$, and $\mu_1 \geq \mu_2 \geq \dots$, and $d = \dim \mathcal{H}_A = \dim \mathcal{H}_B$. It follows from Nielsen's theorem that the state $|\psi'_{AB}\rangle$ may be transformed by LOCC into the maximally entangled state $|\Phi_M^+\rangle$ of Schmidt rank

$$M = \lfloor 2^\gamma \text{Tr } Q \rho_A \rfloor, \quad (56)$$

as the eigenvalues all obey the inequality in (55). This concludes the protocol.

For some $\gamma' > 0$ we can therefore bound the probability of failure of the protocol as follows:

$$\begin{aligned} P_{fail} &= \text{Tr } \overline{Q} \rho_A = \text{Tr } \left[\overline{Q} \left(\rho_A - 2^{-\gamma'} \mathbb{1}_A \right) \right] + 2^{-\gamma'} \text{Tr } \overline{Q} \mathbb{1}_A \\ &\leq \text{Tr } \left(\rho_A - 2^{-\gamma'} \mathbb{1}_A \right)_+ + 2^{-(\gamma' - \gamma)}, \end{aligned}$$

where the inequality follows from the fact that $\text{Tr } \overline{Q} \leq 2^\gamma$ (see Lemma 3.3). Choosing $\gamma = \gamma' + \log \eta$ for some arbitrary $\eta > 0$, and

$$\gamma' = \underline{H}_s^{\varepsilon - \eta}(\rho_A),$$

we obtain

$$P_{fail} = \text{Tr } \overline{Q} \rho_A \leq \varepsilon - \eta + \eta = \varepsilon. \quad (57)$$

Moreover, it follows from (56) that for this choice of γ we have

$$\begin{aligned} \log M &= \gamma + \log(\text{Tr } Q \rho_A) - \Delta \\ &\geq \underline{H}_s^{\varepsilon - \eta}(\rho_A) + \log \eta + \log(1 - \varepsilon) - \Delta, \end{aligned}$$

where Δ is a constant included to ensure that $\log M$ is the logarithm of an integer, and the inequality follows from the fact that

$$\text{Tr } Q \rho_A = 1 - \text{Tr } \overline{Q} \rho_A \geq 1 - \varepsilon,$$

since we have from (57) that $\text{Tr } \overline{Q} \rho_A \leq \varepsilon$. □

Proof of the upper bound in Theorem 5.14 (Converse). To prove the upper bound, we need to establish that if Λ is any LOCC operation such that

$$\log M > -\overline{H}_s^{\varepsilon+\eta}(A|B)_\psi + \delta - \log \eta, \quad (58)$$

then we necessarily have $F(\Lambda(\psi_{AB}), \Phi_M^+) < 1 - \varepsilon$.

To this end, fix $\varepsilon > 0$ and let $\gamma > 0$ be an arbitrary constant. Further, let $\sigma_{AB} := \Lambda(\psi_{AB})$, where Λ is the LOCC operation used in the protocol. Then

$$\begin{aligned} F(\Lambda(\psi_{AB}), \Phi_M^+) &= \langle \Phi_M^+ | \Lambda(\psi_{AB}) | \Phi_M^+ \rangle \\ &= \text{Tr} [\Phi_M^+ (\sigma_{AB} - 2^{-\gamma}(\mathbf{1}_A \otimes \sigma_B))] + 2^{-\gamma} \text{Tr} [\Phi_M^+ (\mathbf{1}_A \otimes \sigma_B)] \\ &\leq \text{Tr} [\{\sigma_{AB} \geq 2^{-\gamma}(\mathbf{1}_A \otimes \sigma_B)\} (\sigma_{AB} \geq 2^{-\gamma}(\mathbf{1}_A \otimes \sigma_B))] \\ &\quad + \text{Tr} [\Phi_M^+ 2^{-\gamma}(\mathbf{1}_A \otimes \sigma_B)] \end{aligned} \quad (59)$$

$$\leq \text{Tr} [\{\sigma_{AB} \geq 2^{-\gamma}(\mathbf{1}_A \otimes \sigma_B)\} (\sigma_{AB} \geq 2^{-\gamma}(\mathbf{1}_A \otimes \sigma_B))] + \frac{2^{-\gamma}}{M}, \quad (60)$$

where the second inequality follows from Lemma 3.1 and the last identity holds because

$$\text{Tr}_A \Phi_M^+ = \frac{\mathbf{1}_A}{M}$$

and σ_B is a normalized state.

Choose

$$\gamma = \overline{H}_s^{\varepsilon+\eta}(A|B)_\sigma - \delta \quad (61)$$

for some arbitrary $\delta > 0$. Then we have

$$-\gamma = -\overline{H}_s^{\varepsilon+\eta}(A|B)_\sigma + \delta \leq -\overline{H}_s^{\varepsilon+\eta}(A|B)_\psi + \delta \quad (62)$$

by Lemma 4.5. We substitute (61) in (60) to obtain

$$\begin{aligned} F(\Lambda(\psi_{AB}), \Phi_M^+) &< 1 - (\varepsilon + \eta) + 2^{-\gamma - \log M} \\ &< 1 - (\varepsilon + \eta) + 2^{\log \eta} \\ &= 1 - \varepsilon, \end{aligned}$$

where the second inequality follows from (58) and (62). This proves the claim. \square

5.3.2 Second order asymptotics of entanglement concentration

The second order asymptotics of entanglement concentration are recorded in the following theorem, where $E_D^{n,\varepsilon}(\psi_{AB})$ is related to the one-shot distillable entanglement via Definition 5.2.

Theorem 5.15. *The second order asymptotic expansion of the distillable entanglement of a pure state ψ_{AB} with error $\varepsilon \in (0, 1)$ is given by*

$$E_D^{n,\varepsilon}(\psi_{AB}) = nS(\rho_A) + \sqrt{n(\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2)} \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n),$$

where $\rho_A = \text{Tr}_B \psi_{AB}$.

Proof. We abbreviate $\rho^n \equiv \rho^{\otimes n}$. From Theorem 5.14 we obtain the following bounds:

$$\underline{H}_s^{\varepsilon-\eta}(\rho_A^n) + \log \eta + \log(1 - \varepsilon) - \Delta \leq E_D^{n,\varepsilon}(\psi_{AB}) \leq -\overline{H}_s^{\varepsilon+\eta}(A^n|B^n)_{\psi^n} + \delta - \log \eta \quad (63)$$

Noting that $\log(1 - \varepsilon) - \Delta = \mathcal{O}(1)$, setting $\eta = \frac{1}{\sqrt{n}}$ and applying Proposition 4.9 to $\underline{H}_s^{\varepsilon-\eta}(\rho_A^n)$, we get

$$\begin{aligned} \underline{H}_s^{\varepsilon-\eta}(\rho_A^n) &= -\overline{D}_s^{\varepsilon-\eta}(\rho_A^n \| \mathbb{1}_{A^n}) \\ &= -nD(\rho_A \| \mathbb{1}_A) + \sqrt{n} \mathfrak{s}(\rho_A \| \mathbb{1}_A) \Phi^{-1}(\varepsilon - \eta) + \mathcal{O}(\log n) \\ &= nS(\rho_A) + \sqrt{n (\text{Tr}[\rho_A(\log \rho_A - \log \mathbb{1}_A)^2] - D(\rho_A \| \mathbb{1}_A)^2)} \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n) \\ &= nS(\rho_A) + \sqrt{n (\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2)} \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n) \end{aligned} \quad (64)$$

where we used Lemma 3.7 in the third equality. For the upper bound in (63) we set $\eta = \frac{1}{\sqrt{n}}$ and apply Proposition 4.9 and Lemma 3.7 to obtain

$$\begin{aligned} -\overline{H}_s^{\varepsilon+\eta}(A^n|B^n)_{\psi^n} &= \underline{D}_s^{\varepsilon+\eta}(\psi_{AB} \| \mathbb{1}_A \otimes \rho_B) \\ &= nD(\psi_{AB} \| \mathbb{1}_A \otimes \rho_B) + \sqrt{n} \mathfrak{s}(\psi_{AB} \| \mathbb{1}_A \otimes \rho_B) \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n) \end{aligned} \quad (65)$$

$$= nS(\rho_A) + \sqrt{n} \mathfrak{s}(\psi_{AB} \| \mathbb{1}_A \otimes \rho_B) \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n). \quad (66)$$

Moreover,

$$\begin{aligned} \mathfrak{s}(\psi_{AB} \| \mathbb{1}_A \otimes \rho_B)^2 &= \text{Tr}[\psi_{AB}(\log \psi_{AB} - \log(\mathbb{1}_A \otimes \rho_B))^2] - D(\psi_{AB} \| \mathbb{1}_A \otimes \rho_B)^2 \\ &= \text{Tr}[\rho_B(\log \rho_B)^2] - S(\rho_A)^2 \\ &= \text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2, \end{aligned} \quad (67)$$

since the first term in the last line only depends on the eigenvalues of ρ_A , which are identical to the eigenvalues of ρ_B . Substituting (67) in (66), we obtain

$$-\overline{H}_s^{\varepsilon+\eta}(A^n|B^n)_{\psi^n} = nS(\rho_A) + \sqrt{n (\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2)} \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n),$$

which, when substituted in (63) together with the lower bound (64), yields the result. \square

5.4 Pure-state entanglement dilution

Pure-state entanglement dilution is the protocol which is essentially opposite to entanglement concentration. Here, the two parties Alice and Bob share a maximally entangled state and wish to convert it into a particular non-maximally entangled state $|\psi_{AB}\rangle$ by LOCC alone.

Suppose Alice and Bob initially share a maximally entangled state $|\Phi_M^+\rangle$ of Schmidt rank M given by (53). Let $\rho_A = \text{Tr}_B \psi_{AB}$, and suppose the Schmidt decomposition of $|\psi_{AB}\rangle$ be given by

$$|\psi_{AB}\rangle = \sum_{k=1}^N \sqrt{\lambda_k} |e_k\rangle \otimes |e_k\rangle, \quad (68)$$

where the Schmidt coefficients λ_k are arranged in non-increasing order, i.e., $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_N$.

Definition 5.16. For any $\varepsilon > 0$, the one-shot ε -error *entanglement cost* of the pure state ψ_{AB} is defined as

$$E_C^{(1),\varepsilon}(\psi_{AB}) := \inf\{\log M \mid \exists \text{ an LOCC map } \Lambda \text{ such that } F(\psi_{AB}, \Lambda(\Phi_M^+)) \geq 1 - \varepsilon\}. \quad \diamond$$

The entanglement cost in the case of asymptotically perfect dilution is known [4] to be given by the entropy of entanglement.

5.4.1 One-shot bounds for pure-state entanglement dilution

We obtain the following one-shot bounds for pure-state entanglement dilution:

Theorem 5.17. *Fix $\varepsilon > 0$ and let $\delta, \eta > 0$. Then the one-shot ε -error entanglement cost of a bipartite pure state ψ_{AB} satisfies the following bounds:*

$$\overline{H}_s^{\varepsilon+\eta}(\rho_A) - \delta + \log \eta \leq E_C^{(1),\varepsilon}(\psi_{AB}) \leq \overline{H}_s^\varepsilon(\rho_A)$$

Proof of the upper bound in Theorem 5.17 (Achievability). Suppose that Alice and Bob share a maximally entangled state of Schmidt rank M given by (53). Alice locally prepares the desired state (68). If $M \geq N$, then the part B of the above state can be teleported to Bob perfectly. However, if $M < N$ then the part B of only the following truncated state can be perfectly teleported:

$$|\psi'_{AB}\rangle := \frac{1}{\text{Tr}(P_M \psi_{AB})} (P_M \otimes \mathbb{1}_B) |\psi_{AB}\rangle, \quad \text{where } (P_M \otimes \mathbb{1}_B) |\psi_{AB}\rangle = \sum_{k=1}^M \sqrt{\lambda_k} |e_k\rangle \otimes |e_k\rangle,$$

that is, P_M denotes the orthogonal projection onto the eigenspace of ρ_A spanned by its M largest eigenvalues. In this case the final state shared between Alice and Bob after the teleportation is given by $|\psi'_{AB}\rangle$. The fidelity of the entanglement dilution protocol in this case is given by

$$\langle \psi_{AB} | \psi'_{AB} | \psi_{AB} \rangle = \sum_{k=1}^M \lambda_k.$$

This simple protocol turns out to be sufficient for proving the upper bound in Theorem 5.17.

In particular, suppose that the final state shared between Alice and Bob after teleportation is given by

$$|\phi_{AB}\rangle := \frac{1}{\text{Tr}[(Q \otimes \mathbb{1}_B) \psi_{AB}]} Q |\psi_{AB}\rangle,$$

where $Q \equiv Q(\gamma)$ is the projection operator given by

$$Q := \{\rho_A \geq 2^{-\gamma} \mathbb{1}_A\},$$

where $\gamma > 0$ and $\rho_A = \text{Tr}_B \psi_{AB}$. Further, note that in order to constitute the final state, we necessarily have

$$\log M = \gamma. \tag{69}$$

This is because the operator Q projects onto the subspace spanned by eigenvectors of ρ_A corresponding to eigenvalues which are less than or equal to $2^{-\gamma}$, and the number of such eigenvalues is at most 2^γ . As the initial maximally entangled state (53) is of Schmidt rank M , perfect teleportation can be achieved if $M = 2^\gamma$, which in turn implies (69).

Choosing $\gamma = \overline{H}_s^\varepsilon(\rho_A)$, it follows from Definition 4.4 of $\overline{H}_s^\varepsilon(\rho_A)$ that we have

$$\text{Tr}(Q \rho_A) \geq \text{Tr} [\{\rho_A \geq 2^{-\gamma} \mathbb{1}_A\} (\rho_A \geq 2^{-\gamma} \mathbb{1}_A)] = 1 - \varepsilon.$$

Hence, denoting the teleportation by Λ , the fidelity of the entanglement dilution protocol can be bounded as follows:

$$\begin{aligned} F(\psi_{AB}, \Lambda(\Phi_M^+)) &= \frac{1}{\text{Tr}[(Q \otimes \mathbb{1}_B) \psi_{AB}]} |\langle \psi_{AB} | (Q \otimes \mathbb{1}_B) | \psi_{AB} \rangle|^2 \\ &= \text{Tr} Q \rho_A \\ &\geq 1 - \varepsilon \end{aligned}$$

Further, from (69) we infer that

$$\log M = \overline{H}_s^\varepsilon(\rho_A) + \delta,$$

which along with Definition 5.16 of the one-shot ε -error entanglement cost implies the upper bound of Theorem 5.17. \square

Proof of the lower bound in Theorem 5.17 (Converse). In order to establish the converse, it suffices to prove that for any entanglement dilution protocol which converts the maximally entangled state $|\Phi_M^+\rangle$ in (53) to the desired state $|\psi_{AB}\rangle$ in (68) with

$$\log M < \overline{H}_s^{\varepsilon+\eta}(\rho_A) - \delta + \log \eta, \quad (70)$$

the fidelity of the entanglement dilution protocol must be strictly less than $1 - \varepsilon$.

Let Λ denote the composite quantum operation realizing the desired entanglement dilution with (70). Then we have

$$\begin{aligned} F(\psi_{AB}, \Lambda(\Phi_M^+)) &= \langle \psi_{AB} | \sum_j (U_j \otimes K_j) |\Phi_M^+\rangle \langle \Phi_M^+| (U_j^\dagger \otimes K_j^\dagger) | \psi_{AB} \rangle, \\ &= \sum_j |\langle \psi_{AB} | (U_j \otimes K_j) |\Phi_M^+\rangle|^2, \end{aligned}$$

where we made use of the Lo-Popescu characterization of LOCC in Lemma 4.5.

Let W be a unitary operator such that $W|e_k\rangle = |\tilde{k}\rangle$ for each $k = 1, 2, \dots, d$. Recall that $\{|e_k\rangle\}$ denotes the Schmidt basis of $|\psi_{AB}\rangle$, whereas $\{|\tilde{k}\rangle\}$ denotes the given orthonormal basis in $\mathcal{H}_A (\simeq \mathcal{H}_B)$ in terms of which the maximally entangled state $|\Phi_M^+\rangle$ has been defined in (53). Further, N is the number of non-zero Schmidt coefficients of $|\psi_{AB}\rangle$. Then, defining the projector $P_M = \sum_{k=1}^M |\tilde{k}_A\rangle \langle \tilde{k}_A|$, we have

$$\begin{aligned} (U_j \otimes \mathbb{1}_B) |\Phi_M^+\rangle &= \frac{1}{\sqrt{M}} \sum_{k=1}^M U_j |\tilde{k}_A\rangle \otimes |\tilde{k}_B\rangle \\ &= \frac{1}{\sqrt{M}} (\mathbb{1}_A \otimes P_M) \sum_{k=1}^N U_j W |k_A\rangle \otimes W |k_B\rangle \\ &= \frac{1}{\sqrt{M}} (\mathbb{1}_A \otimes P_B) \sum_{k=1}^N |k_A\rangle \otimes (U_j W)^T W |k_B\rangle, \\ &= \frac{1}{\sqrt{M}} (\mathbb{1}_A \otimes P_B) \sum_{k=1}^N |k_A\rangle \otimes V_j |k_B\rangle, \end{aligned}$$

where we have defined $V_j = (U_j W)^T W$ and used the fact that

$$\sum_k U |k\rangle \otimes |k\rangle = \sum_k |k\rangle \otimes U^T |k\rangle.$$

Then, using the the Schmidt decomposition (68) of $|\psi_{AB}\rangle$, we obtain

$$\begin{aligned} \langle \psi_{AB} | (U_j \otimes K_j) |\Phi_M^+\rangle &= \sum_k \sqrt{\frac{\lambda_k}{M}} \langle e_k | K_j P_M V_j | e_k \rangle \\ &= \text{Tr} \left(\frac{1}{\sqrt{M}} \sqrt{\rho_A} K_j P_M V_j \right). \end{aligned}$$

Using the Cauchy-Schwarz inequality, we further obtain

$$\begin{aligned}
F(\psi_{AB}, \Lambda(\Phi_M^+)) &= \sum_k \left| \text{Tr} \left(\frac{1}{\sqrt{M}} \sqrt{\rho_A} K_j P_M V_j \right) \right|^2 \\
&= \sum_k \left| \text{Tr} \left(\frac{1}{\sqrt{M}} \sqrt{\rho_A} K_j P_M \cdot P_M V_j \right) \right|^2 \\
&\leq \frac{1}{M} \text{Tr}(P_M) \max_j \text{Tr}(V_j^\dagger P_M V_j \rho_A) \\
&= \frac{1}{M} \text{Tr}(P_M) \max_j \text{Tr}(P_j \rho_A), \\
&= \max_j \text{Tr}(P_j \rho_A),
\end{aligned} \tag{71}$$

where we have defined $P_j = V_j^\dagger P_M V_j$ and used the fact that $\text{Tr} P_M = M$.

Using Lemma 3.1 we have, for any $\gamma > 0$ that

$$\begin{aligned}
\text{Tr} P_j \rho_A &= \text{Tr} [P_j (\rho_A - 2^{-\gamma} \mathbb{1}_A)] + 2^{-\gamma} \text{Tr} P_j, \\
&\leq \text{Tr} [\{(\rho_A \geq 2^{-\gamma} \mathbb{1}_A)\} (\rho_A - 2^{-\gamma} \mathbb{1}_A)] + 2^{-\gamma} \text{Tr} P_j, \\
&= \text{Tr} [\{(\rho_A \geq 2^{-\gamma} \mathbb{1}_A)\} (\rho_A - 2^{-\gamma} \mathbb{1}_A)] + 2^{-\gamma} M,
\end{aligned} \tag{72}$$

since by the cyclicity of the trace and the unitarity of the operators V_j we have

$$\text{Tr} P_j = \text{Tr} V_j^\dagger P_M V_j = \text{Tr} P_M = M.$$

Choose

$$\gamma = \overline{H}_s^{\varepsilon+\eta}(\rho_A) - \delta \tag{73}$$

for some arbitrary $\delta, \eta > 0$. Then using (72) in (71) and substituting in (73) yields

$$\begin{aligned}
F(\psi_{AB}, \Lambda(\Phi_M^+)) &< 1 - (\varepsilon + \eta) + 2^{-\gamma + \log M} \\
&< 1 - (\varepsilon + \eta) + 2^{\log \eta} \\
&= 1 - \varepsilon,
\end{aligned}$$

where we used (70) in the second inequality. This concludes the proof of the converse bound of Theorem 5.17. \square

5.4.2 Second order asymptotics for pure-state entanglement dilution

We obtain the following second order asymptotic expansion for entanglement dilution, where $E_C^{n,\varepsilon}(\psi_{AB})$ is related to the one-shot entanglement cost via Definition 5.2.

Theorem 5.18. *Let ψ_{AB} be a pure bipartite state. For any $\varepsilon \in (0, 1)$, the second order asymptotic expansion of $E_C^{n,\varepsilon}(\psi_{AB})$ is given by*

$$E_C^{n,\varepsilon}(\psi_{AB}) = nS(\rho_A) - \sqrt{n(\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2)} \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n),$$

where $\rho_A = \text{Tr}_B \psi_{AB}$.

Proof. We abbreviate $\rho_A^n \equiv \rho_A^{\otimes n}$. By Theorem 5.17 we have the following one-shot bounds for finite block length size:

$$\overline{H}_s^{\varepsilon+\eta}(\rho_A^n) - \delta + \log \eta \leq E_C^{n,\varepsilon}(\psi_{AB}) \leq \overline{H}_s^{\varepsilon}(\rho_A^n) \quad (74)$$

We apply Proposition 4.9 to $\overline{H}_s^{\varepsilon}(\rho_A^n)$ to obtain

$$\begin{aligned} \overline{H}_s^{\varepsilon}(\rho_A^n) &= -nD(\rho_A \| \mathbb{1}_A) - \sqrt{n} \mathfrak{s}(\rho_A \| \mathbb{1}_A) \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n) \\ &= nS(\rho_A) - \sqrt{n(\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2)} \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n) \end{aligned} \quad (75)$$

For the lower bound in (74) we set $\eta = \frac{1}{\sqrt{n}}$ and apply (75) and Lemma 3.7, which finally yields the claim. \square

The converse bound in Theorem 5.17 together with the asymptotic expansion for entanglement dilution in Theorem 5.18 implies the following result, which we employ in the next section:

Corollary 5.19. *Let $\delta > 0$ and n be sufficiently large. For any LOCC map \mathcal{D}_n used in an entanglement dilution protocol, for which*

$$F(\psi_{AB}^{\otimes n}, \mathcal{D}_n(\Phi_{M_n}^+)) \geq 1 - \delta,$$

the Schmidt rank M_n of the MES $\Phi_{M_n}^+$ must satisfy

$$\log M_n \geq nS(\rho_A) - \sqrt{n(\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2)} \Phi^{-1}(\delta) + \mathcal{O}(\log n).$$

5.5 Irreversibility of entanglement concentration

In the asymptotic limit, the distillable entanglement for any given bipartite pure state ψ_{AB} is equal to its entanglement cost, and is given by the *entropy of entanglement* $S(\rho_A)$ (where $\rho_A = \text{Tr}_B \psi_{AB}$). This equality between the optimal rates of asymptotically perfect entanglement concentration and entanglement dilution has led to the popular belief that entanglement conversions of pure bipartite states are *asymptotically reversible*. The reversibility is in the sense that, in the asymptotic limit, the ebits extracted from multiple copies of ψ_{AB} via entanglement concentration can subsequently be used to recover the original number of copies of the state ψ_{AB} via entanglement dilution. However, recently Kumagai and Hayashi [28] proved that the error incurred in the composite process (i.e. concentration followed by dilution) is necessarily non-zero, even in the asymptotic limit. This implies that, contrary to popular belief, entanglement concentration is in fact irreversible.

Second order asymptotic expansions for the distillable entanglement and the entanglement cost (as given by Theorem 5.15 and Theorem 5.18 respectively) show that even though to leading order the number of ebits which can be distilled from $\psi_{AB}^{\otimes n}$ is equal to the number of ebits needed to create $\psi_{AB}^{\otimes n}$, there is a discrepancy between these two quantities in the second order (\sqrt{n}). In this section we show how the irreversibility of entanglement concentration can be easily proved using this discrepancy. We formalize the concept of (ir-)reversibility in the following way:

Definition 5.20.

- (i) Set $M_n = \lfloor \exp(nS(\rho_A)) \rfloor$. A sequence $\{\mathcal{C}_n\}_{n \in \mathbb{N}}$ of LOCC maps, where $\mathcal{C}_n : \mathcal{D}(\mathcal{H}_{AB}^{\otimes n}) \rightarrow \mathcal{D}(\mathcal{H}_{AB}^{\otimes n})$, is called an *asymptotically perfect concentration protocol* (APCP), if it converts the sequence of pure states $\{\psi_{AB}^{\otimes n}\}_{n \in \mathbb{N}}$ to the sequence of MES $\{\Phi_{M_n}^+\}_{n \in \mathbb{N}}$ with asymptotically vanishing error, that is, for any $\varepsilon > 0$ there exists an $N \in \mathbb{N}$ such that for all $n > N$ we have

$$F(\mathcal{C}_n(\psi_{AB}^{\otimes n}), \Phi_{M_n}^+) \geq 1 - \varepsilon.$$

This is equivalent to $\lim_{n \rightarrow \infty} F(\mathcal{C}_n(\psi_{AB}^{\otimes n}), \Phi_{M_n}^+) = 1$.

(ii) We say that entanglement concentration is *reversible* if

$$\lim_{n \rightarrow \infty} \max_{\mathcal{D}_n} F(\psi_{AB}^{\otimes n}, (\mathcal{D}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n})) = 1$$

where $\{\mathcal{C}_n\}_{n \in \mathbb{N}}$ is a sequence of APCPs and the minimization is over all sequences of LOCC maps $\{\mathcal{D}_n\}_{n \in \mathbb{N}}$, with $\mathcal{D}_n : \mathcal{D}(\mathcal{H}_{AB}^{\otimes n}) \rightarrow \mathcal{D}(\mathcal{H}_{AB}^{\otimes n})$, used in the entanglement dilution protocol. \diamond

Theorem 5.21. *Entanglement concentration of any given bipartite pure state ψ_{AB} is irreversible, i.e. for any sequence $\{\mathcal{C}_n\}_{n \in \mathbb{N}}$ of APCPs we have*

$$\lim_{n \rightarrow \infty} \max_{\mathcal{D}_n : \text{LOCC}} F(\psi_{AB}^{\otimes n}, (\mathcal{D}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n})) < 1.$$

Proof. Let $\{\mathcal{C}_n\}_{n \in \mathbb{N}}$ be a sequence of APCPs as in Definition 5.20 and fix $\varepsilon \in (0, \frac{1}{2})$. By our result on the second order asymptotics for entanglement concentration (Theorem 5.14), for sufficiently large n we have

$$\begin{aligned} \log M_n &= nS(\rho_A) + \sqrt{n(\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2)} \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n) \\ &\equiv nS(\rho_A) + \sqrt{n(\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2)} \Phi^{-1}(\varepsilon) + f(n) \end{aligned} \quad (76)$$

where in the second line f is a function satisfying $\lim_{n \rightarrow \infty} (f(n)/\sqrt{n}) = 0$, which can be chosen since $\mathcal{O}(\log n) \subset o(\sqrt{n})$. Contrarily, Corollary 5.19 implies that for every dilution protocol \mathcal{D}_n with

$$F(\psi_{AB}^{\otimes n}, \mathcal{D}_n(\Phi_{M'_n}^+)) \geq 1 - \delta,$$

where $\delta > 0$ and n is sufficiently large, the Schmidt rank M'_n of the initially shared MES $\Phi_{M'_n}^+$ must satisfy

$$\begin{aligned} \log M'_n &\geq nS(\rho_A) - \sqrt{n(\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2)} \Phi^{-1}(\delta) + \mathcal{O}(\log n) \\ &\equiv nS(\rho_A) - \sqrt{n(\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2)} \Phi^{-1}(\delta) + g(n). \end{aligned} \quad (77)$$

Here, g is chosen such that $\lim_{n \rightarrow \infty} (g(n)/\sqrt{n}) = 0$. We show in the following that (76) does not satisfy this bound. For $\delta, \varepsilon > (0, \frac{1}{2})$ we have that $\Phi^{-1}(\varepsilon)$ and $\Phi^{-1}(\delta)$ are strictly negative. Note that the restriction of both ε and δ to the interval $(0, \frac{1}{2})$ arises from the requirement that the overall error of the recovery process can be at most 1.

Subtracting the expression for $\log M_n$ given by (76) from the RHS of (77) yields

$$\sqrt{n} \left(-\sqrt{\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2} (\Phi^{-1}(\delta) + \Phi^{-1}(\varepsilon)) + \frac{g(n) - f(n)}{\sqrt{n}} \right). \quad (78)$$

Since $\lim_{n \rightarrow \infty} \frac{g(n) - f(n)}{\sqrt{n}} = 0$, we can make this term arbitrarily small for sufficiently large n , that is,

$$\left| \frac{g(n) - f(n)}{\sqrt{n}} \right| < -\sqrt{\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2} (\Phi^{-1}(\delta) + \Phi^{-1}(\varepsilon)),$$

and hence the difference in (78) is strictly positive, yielding

$$\log M_n < nS(\rho_A) - \sqrt{n(\text{Tr}[\rho_A(\log \rho_A)^2] - S(\rho_A)^2)} \Phi^{-1}(\delta) + g(n)$$

for sufficiently large n . Therefore, $F(\psi_{AB}^{\otimes n}, \mathcal{D}_n(\Phi_{M'_n}^+)) < 1 - \delta$, and, using the inequality $\sqrt{1-x} \leq 1 - \frac{x}{2}$, this implies

$$\sqrt{F(\psi_{AB}^{\otimes n}, \mathcal{D}_n(\Phi_{M'_n}^+))} < 1 - \frac{\delta}{2}. \quad (79)$$

Using the trace distance $d(.,.)$ we now compute:

$$\begin{aligned}
\frac{\delta}{2} &< 1 - \sqrt{F(\psi_{AB}^{\otimes n}, \mathcal{D}_n(\Phi_{M_n}^+))} \\
&\leq d(\psi_{AB}^{\otimes n}, \mathcal{D}_n(\Phi_{M_n}^+)) \\
&\leq d(\psi_{AB}^{\otimes n}, (\mathcal{D}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n})) + d((\mathcal{D}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n}), \mathcal{D}_n(\Phi_{M_n}^+)) \\
&\leq d(\psi_{AB}^{\otimes n}, (\mathcal{D}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n})) + d(\mathcal{C}_n(\psi_{AB}^{\otimes n}), \Phi_{M_n}^+), \tag{80}
\end{aligned}$$

where the first inequality follows from (79), the second inequality is the Fuchs-van-de-Graaf inequality [14], the third inequality is the triangle inequality for the trace distance and the fourth inequality follows from the monotonicity of the trace distance under CPTP maps. Applying the Fuchs-van-de-Graaf-inequality to the term $d(\mathcal{C}_n(\psi_{AB}^{\otimes n}), \Phi_{M_n}^+)$, we obtain

$$1 - \sqrt{F(\mathcal{C}_n(\psi_{AB}^{\otimes n}), \Phi_{M_n}^+)} \leq d(\mathcal{C}_n(\psi_{AB}^{\otimes n}), \Phi_{M_n}^+) \leq \sqrt{1 - F(\mathcal{C}_n(\psi_{AB}^{\otimes n}), \Phi_{M_n}^+)}$$

and consequently,

$$\lim_{n \rightarrow \infty} d(\mathcal{C}_n(\psi_{AB}^{\otimes n}), \Phi_{M_n}^+) = 0 \tag{81}$$

since $\lim_{n \rightarrow \infty} F(\mathcal{C}_n(\psi_{AB}^{\otimes n}), \Phi_{M_n}^+) = 1$ by Definition 5.20 of the APCP $\{\mathcal{C}_n\}_{n \in \mathbb{N}}$. Therefore, for any sequence of LOCC maps $\{\mathcal{D}_n\}_{n \in \mathbb{N}}$, we have by (80) and (81) that

$$\lim_{n \rightarrow \infty} d(\psi_{AB}^{\otimes n}, (\mathcal{D}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n})) > \frac{\delta}{2}.$$

Choose the sequence $\{\tilde{\mathcal{D}}_n\}_{n \in \mathbb{N}}$ such that

$$\max_{\mathcal{D}_n} F(\psi_{AB}^{\otimes n}, (\mathcal{D}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n})) = F(\psi_{AB}^{\otimes n}, (\tilde{\mathcal{D}}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n})).$$

Then, by another application of the Fuchs-van-de-Graaf inequality, we obtain

$$\begin{aligned}
\frac{\delta}{2} &< \lim_{n \rightarrow \infty} d(\psi_{AB}^{\otimes n}, (\tilde{\mathcal{D}}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n})) \\
&\leq \lim_{n \rightarrow \infty} \sqrt{1 - F(\psi_{AB}^{\otimes n}, (\tilde{\mathcal{D}}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n}))} \\
&= \sqrt{1 - \lim_{n \rightarrow \infty} F(\psi_{AB}^{\otimes n}, (\tilde{\mathcal{D}}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n}))} \\
&= \sqrt{1 - \lim_{n \rightarrow \infty} \max_{\mathcal{D}_n} F(\psi_{AB}^{\otimes n}, (\mathcal{D}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n}))},
\end{aligned}$$

which yields

$$\lim_{n \rightarrow \infty} \max_{\mathcal{D}_n} F(\psi_{AB}^{\otimes n}, (\mathcal{D}_n \circ \mathcal{C}_n)(\psi_{AB}^{\otimes n})) < 1 - \frac{\delta^2}{4} < 1,$$

since δ is strictly positive. This proves the claim. \square

5.6 Classical-quantum channels

The transmission of information through classical-quantum (c-q) channels has been studied by various authors. Wang and Renner [49] obtained bounds on the one-shot capacity in terms of the hypothesis testing relative entropy, whereas in [11] the bounds were expressed in terms of the smooth max-relative entropy. Both these sets of bounds converged to the Holevo capacity [22, 43] in the asymptotic i.i.d. limit. However, [11] had the advantage of also yielding the strong converse property of the Holevo capacity. The latter ensures that for transmission rates above the Holevo capacity, information transmission fails with certainty. This was originally proved by Ogawa and Nagaoka [36], and independently by Winter [50].

More recently, in [48], Tomamichel and Tan derived the second order asymptotics of the capacity of a c-q channel, starting from one-shot bounds expressed in terms of the hypothesis testing relative entropy. Here we obtain one-shot bounds in terms of an information spectrum relative entropy, and then use its second order asymptotic expansion to recover the result of Tomamichel and Tan [48]. Like [11] and [47], our result too has the advantage of yielding the strong converse property of the Holevo capacity, in addition to the direct and weak converse parts of the HSW theorem [22, 43].

Consider a classical-quantum channel $W : \mathcal{X} \rightarrow \mathcal{D}(\mathcal{H}_B)$, where \mathcal{H}_B is a finite-dimensional Hilbert space, and \mathcal{X} denotes the (finite) input alphabet. Suppose that Alice (the sender) wants to communicate with Bob (the receiver) using the channel W . To do this, they agree on a finite set of possible messages, labelled by natural numbers from 1 to M . To send the message labelled by $m \in \{1, \dots, M\}$, Alice has to encode her message into an input signal of the channel, $\varphi(m) \in \mathcal{X}$, and send it through the channel W , resulting in the quantum state $W(\varphi(m))$ at Bob's side. Bob then performs a POVM (positive operator-valued measure) $\Pi := \{\Pi_i\}_{i=1}^M$, and if the outcome corresponding to Π_k happens, he concludes that the message with label k was sent. The probability of this event is $\text{Tr}[W(\varphi(m))\Pi_k]$. A triple $\mathcal{C} = (M, \varphi, \Pi)$ defines a code, where:

- $M \in \mathbb{N}$ is the number of possible messages.
- $\varphi : \{1, 2, \dots, M\} \rightarrow \mathcal{X}$ is Alice's encoding of possible messages into input signals of the channel.
- $\Pi := \{\Pi_m\}_{m=1}^M$ (with $\Pi_m \geq 0 \ \forall m = 1, 2, \dots, M$, and $\sum_{m=1}^M \Pi_m = I$) is a POVM on \mathcal{H}_B , performed by Bob to identify the message (decoding).

The *average error probability* $p_e(\mathcal{C}, W)$ of a code $\mathcal{C} = (M, \varphi, \Pi)$ is defined as

$$p_e(\mathcal{C}, W) := \frac{1}{M} \sum_{i=1}^M (1 - \text{Tr}[W(\varphi(i))\Pi_i]). \quad (82)$$

Definition 5.22. For a given $\varepsilon > 0$, the *one-shot ε -error capacity* $C_\varepsilon^{(1)}(W)$ of a channel W is defined as

$$C_\varepsilon^{(1)}(W) := \sup\{\log M \mid \exists \text{ a code } \mathcal{C} = (M, \varphi, \Pi) \text{ such that } p_e(\mathcal{C}, W) \leq \varepsilon\}. \quad \diamond$$

Note that it quantifies the maximum number of bits that can be transmitted through a single use of the channel with an average error probability of at most ε .

5.6.1 One-shot bounds for c-q channels

Our aim is to give bounds on $C_\varepsilon^{(1)}(W)$ in terms of the information spectrum mutual information. For the input alphabet \mathcal{X} , let $\mathcal{P}(\mathcal{X})$ denote the set of probability distributions on \mathcal{X} . Further, let $\mathcal{H}_\mathcal{X}$ be a Hilbert space with $\dim \mathcal{H}_\mathcal{X} = |\mathcal{X}|$ and an orthonormal basis $\{|x\rangle\}_{x \in \mathcal{X}}$. For any probability distribution $p = \{p(x)\}_{x \in \mathcal{X}} \in \mathcal{P}(\mathcal{X})$, consider the classical-quantum (c-q) state

$$\rho_{XB}(p) := \sum_{x \in \mathcal{X}} p(x) |x\rangle\langle x| \otimes W(x) \quad \text{with } p \in \mathcal{P}(\mathcal{X}). \quad (83)$$

Its reduced states are given by $\rho_B = \sum_{x \in \mathcal{X}} p(x) W(x)$ and

$$\rho_X(p) := \text{Tr}_B \rho_{XB}(p) = \sum_{x \in \mathcal{X}} p(x) |x\rangle\langle x|.$$

Theorem 5.23. Fix $\varepsilon > 0$, $\delta, c > 0$ and let $\eta > \frac{c}{c+1}\varepsilon$. Then the one-shot ε -error capacity of a c-q channel $W : \mathcal{X} \rightarrow \mathcal{D}(\mathcal{H}_B)$ satisfies the following bounds:

$$C_\varepsilon^{(1)}(W) \geq \max_{p \in \mathcal{P}(\mathcal{X})} \underline{D}_s^{\varepsilon-\eta}(\rho_{XB} \| \rho_X \otimes \rho_B) + \log \frac{c}{1+c} + \log \left(\eta - \frac{c}{1+c}\varepsilon \right) \quad (84)$$

$$C_\varepsilon^{(1)}(W) \leq \max_{p \in \mathcal{P}(\mathcal{X})} \min_{\sigma_B} \underline{D}_s^{\varepsilon+\eta}(\rho_{XB} \| \rho_X \otimes \sigma_B) + \delta - \log \eta, \quad (85)$$

where $\rho_{XB} = \rho_{XB}(p)$ with $p \in \mathcal{P}(\mathcal{X})$ as defined in (83).

Proof of the lower bound in Theorem 5.23 (Achievability). To establish the lower bound in (84) of Theorem 5.23, we again make use of Lemma 5.1 by Hayashi and Nagaoka. First, let $p = \{p(x)\}_{x \in \mathcal{X}} \in \mathcal{P}(\mathcal{X})$ denote the probability distribution for which the maximum in the lower bound of (84) holds, and let $\rho_{XB} \equiv \rho_{XB}(p)$. For any $\gamma > 0$, define the difference operator

$$\begin{aligned} \Pi(\gamma) &= \rho_{XB} - 2^\gamma \rho_X \otimes \rho_B \\ &= \sum_{x \in \mathcal{X}} p(x) |x\rangle\langle x| \otimes (W(x) - 2^\gamma \overline{W}), \end{aligned}$$

where $\overline{W} = \sum_{x \in \mathcal{X}} p(x) W(x)$. Then

$$\begin{aligned} \alpha &:= \text{Tr} [\{\Pi(\gamma) \geq 0\} \Pi(\gamma)] \\ &= \sum_{x \in \mathcal{X}} p(x) \text{Tr} [\{W(x) \geq 2^\gamma \overline{W}\} (W(x) - 2^\gamma \overline{W})]. \end{aligned}$$

Fix $c > 0$ and $\eta > \frac{c}{1+c}\varepsilon$. Choose

$$\gamma = \underline{D}_s^{\varepsilon-\eta}(\rho_{XB} \| \rho_X \otimes \rho_B),$$

with $\rho_{XB} \equiv \rho_{XB}(p)$ for the optimizing distribution $p \in \mathcal{P}(\mathcal{X})$ chosen above. For this choice of γ we have $\alpha \geq 1 - (\varepsilon - \eta)$. Then Lemma 5.1 implies the existence of a code \mathcal{C} of size M such that for any $c > 0$,

$$\begin{aligned} p_e(\mathcal{C}) &\leq (1+c)(1-\alpha) + (2+c+c^{-1})2^{-\gamma}M \\ &\leq (1+c)(\varepsilon-\eta) + (2+c+c^{-1})2^{-\gamma}M. \end{aligned}$$

Thus $p_e(\mathcal{C}) \leq \varepsilon$ for the choice of M such that

$$(1+c)(\varepsilon-\eta) + \frac{(1+c)^2}{c} 2^{-\gamma} M = \varepsilon,$$

that is, for

$$\begin{aligned}\log M &= \gamma + \log \frac{c}{1+c} + \log \left(\eta - \frac{c}{1+c} \varepsilon \right) \\ &= \underline{D}_s^{\varepsilon-\eta}(\rho_{XB} \| \rho_X \otimes \rho_B) + \log \frac{c}{1+c} + \log \left(\eta - \frac{c}{1+c} \varepsilon \right).\end{aligned}\quad (86)$$

Note that the argument of the right-most logarithm yields the condition $\eta > \frac{c}{c+1} \varepsilon$. Definition 5.22 of the one-shot ε -error capacity along with (86) implies the lower (achievability) bound (84). \square

Proof of the upper bound in Theorem 5.23 (Converse). To establish the upper bound in (85) in Theorem 5.23, it suffices to prove that for any code \mathcal{C} of M codewords with

$$\log M > \max_{p \in \mathcal{P}(\mathcal{X})} \min_{\sigma_B} \underline{D}_s^{\varepsilon+\eta}(\rho_{XB} \| \rho_X \otimes \sigma_B) + \delta - \log \eta \quad (87)$$

we must have $p_e(\mathcal{C}) > \varepsilon$.

We make the following definitions: Let $\mathcal{C} = (M, \varphi, \Pi)$ be a code such that (87) holds and $x_m = \varphi(m)$, $m = 1, \dots, M$ be the codewords. Let $\rho_m = W(x_m)$ be the output states of the channel and let $p \in \mathcal{P}(\mathcal{X})$ be the uniform distribution on the codewords, i.e., $p(x) = 1/M$ if $x = x_m$ for some $m = 1, \dots, M$, and $p(x) = 0$ otherwise. Further, let $\bar{\rho} := \frac{1}{M} \sum_{m=1}^M \rho_m$. For the chosen p , we define

$$\tilde{\rho}_{XB} := \rho_{XB}(p) = \frac{1}{M} \sum_{m=1}^M |x_m\rangle\langle x_m| \otimes \rho_m. \quad (88)$$

Let σ_B be the state for which

$$\underline{D}_s^{\varepsilon+\eta}(\tilde{\rho}_{XB} \| \tilde{\rho}_X \otimes \sigma_B) = \min_{\sigma'_B} \underline{D}_s^{\varepsilon+\eta}(\tilde{\rho}_{XB} \| \tilde{\rho}_X \otimes \sigma'_B);$$

then we obtain

$$\begin{aligned}p_e(\mathcal{C}) &:= 1 - \frac{1}{M} \sum_{m=1}^M \text{Tr} \Pi_m \rho_m \\ &= 1 - \frac{1}{M} \sum_{m=1}^M \text{Tr} [\Pi_m (\rho_m - 2^\gamma \sigma_B)] - \frac{2^\gamma}{M} \sum_{m=1}^M \text{Tr} \Pi_m \sigma_B \\ &\geq 1 - \frac{1}{M} \sum_{m=1}^M \text{Tr} [\{\rho_m \geq 2^\gamma \sigma_B\} (\rho_m - 2^\gamma \sigma_B)] - \frac{2^\gamma}{M},\end{aligned}\quad (89)$$

where we used Lemma 3.1 in the last inequality. Choose

$$\begin{aligned}\gamma &= \max_{p \in \mathcal{P}(\mathcal{X})} \min_{\sigma_B} \underline{D}_s^{\varepsilon+\eta}(\rho_{XB} \| \rho_X \otimes \sigma_B) + \delta \\ &= \max_{p \in \mathcal{P}(\mathcal{X})} \underline{I}_s^{\varepsilon+\eta}(X : B)_\rho + \delta\end{aligned}\quad (90)$$

$$\geq \underline{I}_s^{\varepsilon+\eta}(X : B)_{\bar{\rho}} + \delta \quad (91)$$

for some arbitrary $\delta > 0$. Here, $\bar{\rho}$ is the c-q state corresponding to the uniform distribution, defined through (88). Hence,

$$\underline{I}_s^{\varepsilon+\eta}(X : B)_{\bar{\rho}} = \sup \left\{ \gamma : \frac{1}{M} \sum_{m=1}^M \text{Tr} (\rho_m - 2^\gamma \sigma_B)_+ \geq 1 - (\varepsilon + \eta) \right\}. \quad (92)$$

Using (91) in (89) yields

$$\begin{aligned} p_e(\mathcal{C}) &> \varepsilon + \eta - 2^{\gamma - \log M} \\ &> \varepsilon + \eta - 2^{\log \eta} \\ &= \varepsilon, \end{aligned}$$

where we used (87) and (90) in the second inequality. \square

5.6.2 Second order asymptotics of c-q channels

In this section we show that our one-shot bounds for the ε -error capacity of a cq-channel from Theorem 5.23 reproduce its second order asymptotics proved in [48, Theorem 10]. Before we state this result precisely, we make the following definitions:

The capacity $C(W)$ of a c-q channel is defined as

$$C(W) = \max_{p \in \mathcal{P}(\mathcal{X})} I(X : B)_\rho$$

with ρ_{XB} as in (83). Furthermore, let Π be the set of probability distributions achieving the maximum in $C(W)$, and define

$$V_{\min} := \min_{p \in \Pi} V(\rho_{XB} \| \rho_X \otimes \rho_B) \quad \text{and} \quad V_{\max} := \max_{p \in \Pi} V(\rho_{XB} \| \rho_X \otimes \rho_B).$$

Then V_ε is defined by

$$V_\varepsilon = \begin{cases} V_{\min} & \text{if } \varepsilon \in (0, \frac{1}{2}) \\ V_{\max} & \text{if } \varepsilon \in [\frac{1}{2}, 1). \end{cases}$$

Proposition 5.24. *Let $\varepsilon \in (0, 1)$ and assume $V_{\min} > 0$. Then the second order expansion of the ε -error capacity $C(n, \varepsilon)$ of a cq-channel W is given by*

$$C(n, \varepsilon) = nC(W) + \sqrt{nV_\varepsilon} \Phi^{-1}(\varepsilon) + o(\sqrt{n}).$$

Proof. Note that the condition $V_{\min} > 0$ implies $V_\varepsilon > 0$. We first prove the bound

$$C(n, \varepsilon) \geq nC(W) + \sqrt{nV_\varepsilon} \Phi^{-1}(\varepsilon) + o(\sqrt{n}). \quad (93)$$

To this end, we write $\rho_{X^n B^n} = \sum_{\mathbf{x} \in \mathcal{X}^n} p(\mathbf{x}) |\mathbf{x}\rangle \langle \mathbf{x}| \otimes W^{(n)}(\mathbf{x})$ where $W^{(n)} : \mathcal{X}^n \rightarrow \mathcal{H}_{B^n}$ and $\mathbf{x} := x_1 \dots x_n$ with $x_i \in \mathcal{X}$, and employ the one-shot lower bound from Theorem 5.23 after n rounds, which reads:

$$\begin{aligned} C(n, \varepsilon) &\geq \max_{p \in P(\mathcal{X}^n)} \underline{D}_s^{\varepsilon - \eta}(\rho_{X^n B^n} \| \rho_{X^n} \otimes \rho_{B^n}) + \log \frac{c}{1+c} + \log \left(\eta - \frac{c}{1+c} \varepsilon \right) \\ &\geq \max_{p \in P(\mathcal{X})} \underline{D}_s^{\varepsilon - \eta}(\rho_{XB}^{\otimes n} \| \rho_X^{\otimes n} \otimes \rho_B^{\otimes n}) + \log \frac{c}{1+c} + \log \left(\eta - \frac{c}{1+c} \varepsilon \right) \end{aligned}$$

Setting $c = \frac{1}{n}$ and choosing $\eta = \frac{1}{\sqrt{n}}$, we apply Proposition 4.9 to obtain

$$\begin{aligned} C(n, \varepsilon) &\geq n \max_{p \in P(\mathcal{X})} D(\rho_{XB} \| \rho_X \otimes \rho_B) + \sqrt{n} \max_{p \in P(\mathcal{X})} s(\rho_{XB} \| \rho_X \otimes \rho_B) \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n) \\ &= nC(W) + \sqrt{n \max_{p \in P(\mathcal{X})} V(\rho_{XB} \| \rho_X \otimes \rho_B)} \Phi^{-1}(\varepsilon) + \mathcal{O}(\log n). \end{aligned}$$

According to the proof of Proposition 11 in [48], we can choose a maximizing distribution $\bar{p} \in P(\mathcal{X})$ such that $V(\rho_{XB} \| \rho_X \otimes \rho_B) = V_\varepsilon$. Since $\mathcal{O}(\log n) \subseteq o(\sqrt{n})$, this yields the lower bound (93).

In order to prove

$$C(n, \varepsilon) \leq nC(W) + \sqrt{nV_\varepsilon} \Phi^{-1}(\varepsilon) + o(\sqrt{n}), \quad (94)$$

we first rewrite the one-shot upper bound

$$C_\varepsilon^{(1)}(W) \leq \max_{p \in \mathcal{P}(\mathcal{X})} \underline{I}_s^{\varepsilon+\eta}(X : B)_\rho + \delta - \log \eta \quad (95)$$

from Theorem 5.23. To this end, let $\bar{\rho}_B^x$ maximize $\max_{x \in \mathcal{X}} \underline{D}_s^{\varepsilon+\eta}(\rho_B^x \| \sigma_B)$. It follows that

$$\begin{aligned} 1 - (\varepsilon + \eta) &\leq \sum_{x \in \mathcal{X}} p(x) \text{Tr}(\rho_B^x - 2^\gamma \sigma_B)_+ \\ &\leq \text{Tr}(\bar{\rho}_B^x - 2^\gamma \sigma_B)_+ \sum_{x \in \mathcal{X}} p(x) \\ &= \text{Tr}(\bar{\rho}_B^x - 2^\gamma \sigma_B)_+, \end{aligned}$$

and hence,

$$\max_{x \in \mathcal{X}} \underline{D}_s^{\varepsilon+\eta}(\rho_B^x \| \sigma_B) \geq \underline{D}_s^{\varepsilon+\eta}(\rho_{XB} \| \rho_X \otimes \sigma_B). \quad (96)$$

We therefore have

$$\begin{aligned} \max_{p \in \mathcal{P}(\mathcal{X})} \underline{I}_s^{\varepsilon+\eta}(X : B)_\rho &= \max_{p \in \mathcal{P}(\mathcal{X})} \min_{\sigma_B} \underline{D}_s^{\varepsilon+\eta}(\rho_{XB} \| \rho_X \otimes \sigma_B) \\ &\leq \min_{\sigma_B} \max_{p \in \mathcal{P}(\mathcal{X})} \underline{D}_s^{\varepsilon+\eta}(\rho_{XB} \| \rho_X \otimes \sigma_B) \\ &\leq \min_{\sigma_B} \max_{x \in \mathcal{X}} \underline{D}_s^{\varepsilon+\eta}(\rho_B^x \| \sigma_B), \end{aligned} \quad (97)$$

where we used (96) in the last inequality. Inserting (97) into (95) yields

$$\begin{aligned} C(n, \varepsilon) &\leq \min_{\sigma_{B^n}} \max_{\mathbf{x} \in \mathcal{X}^n} \underline{D}_s^{\varepsilon+\eta}(\rho_B^{\mathbf{x}} \| \sigma_{B^n}) + \delta - \log \eta \\ &\leq \min_{\sigma_{B^n}} \max_{\mathbf{x} \in \mathcal{X}^n} D_H^{\varepsilon+\eta}(\rho_B^{\mathbf{x}} \| \sigma_{B^n}) + \delta - \log \eta. \end{aligned}$$

with the second inequality following from the bound $\underline{D}_s^\varepsilon(\rho \| \sigma) \leq D_H^\varepsilon(\rho \| \sigma)$ in Proposition 4.7(i). We finally apply the reasoning in the proof of Proposition 13 in [48] to the term

$$\min_{\sigma_{B^n}} \max_{\mathbf{x} \in \mathcal{X}^n} D_H^{\varepsilon+\eta}(\rho_B^{\mathbf{x}} \| \sigma_{B^n})$$

and set $\eta = \frac{1}{\sqrt{n}}$ to arrive at (94). \square

6 Optimal rates for the case of arbitrary resources

The information spectrum approach (ISA) allows us to obtain expressions for optimal rates of information-processing tasks involving arbitrary sources, channels and entanglement resources.. That is, the assumption for the resources employed in the protocols being memoryless (or i.i.d.) is not imposed. As mentioned earlier, the central quantities in the ISA are the spectral divergence rates $\underline{D}(\hat{\rho} \| \hat{\omega})$ and $\overline{D}(\hat{\rho} \| \hat{\omega})$ defined in eqs.(17) and (18) respectively. Here, $\hat{\rho} = \{\rho_n\}_{n \in \mathbb{N}}$ denotes an arbitrary sequence of states and $\hat{\omega} = \{\omega_n\}_{n \in \mathbb{N}}$ denotes an arbitrary sequence of positive semi-definite operators, with $\rho_n, \omega_n \in \mathcal{B}(\mathcal{H}^{\otimes n})$. Further, the following entropic quantities are derived from them:

- (i) The quantum inf- and sup-spectral entropy rates

$$\underline{S}(\hat{\rho}) := -\overline{D}(\hat{\rho}||\hat{I}) \quad \text{and} \quad \overline{S}(\hat{\rho}) := -\underline{D}(\hat{\rho}||\hat{I}),$$

where $\hat{I} = \{I_n\}_{n \in \mathbb{N}}$ denotes a sequence of identity operators, with $I_n \in \mathcal{B}(\mathcal{H}^{\otimes n})$.

- (ii) The inf- and sup-spectral conditional entropy rates for an arbitrary sequence of bipartite states $\hat{\rho}_{AB} := \{\rho_{AB}^n\}_{n \in \mathbb{N}}$:

$$\underline{S}(A|B)_{\hat{\rho}} := -\overline{D}(\hat{\rho}_{AB}||\hat{1}_A \otimes \hat{\rho}_B) \quad \text{and} \quad \overline{S}(A|B)_{\hat{\rho}} := -\underline{D}(\hat{\rho}_{AB}||\hat{1}_A \otimes \hat{\rho}_B),$$

where $\hat{\rho}_B = \{\rho_B^n\}_{n \in \mathbb{N}}$, with ρ_B^n denoting the reduced state of the state ρ_{AB}^n .

- (iii) The inf- and sup-spectral mutual information rates for sequences of bipartite states $\hat{\rho}_{AB} := \{\rho_{AB}^n\}_{n \in \mathbb{N}}$:

$$\underline{I}(A : B)_{\hat{\rho}} := \underline{D}(\hat{\rho}_{AB}||\hat{\rho}_A \otimes \hat{\rho}_B) \quad \text{and} \quad \overline{I}(A : B)_{\hat{\rho}} := \overline{D}(\hat{\rho}_{AB}||\hat{\rho}_A \otimes \hat{\rho}_B).$$

Starting from our one-shot bounds for the various tasks studied in this paper, we can directly recover the known expressions for corresponding optimal rates for the case of arbitrary resources, as obtained in the ISA. This is done by employing the relations between the information spectrum relative entropies and the spectral divergence rates proved in Proposition 4.12. For the tasks considered in this paper, the rates in the ISA are defined as follows:

Definition 6.1.

- (i) For a general quantum information source characterized by an arbitrary sequence of states $\hat{\rho} = \{\rho_n\}_{n \in \mathbb{N}}$ acting on a corresponding sequence of Hilbert spaces $\hat{\mathcal{H}} = \{\mathcal{H}_n\}_{n \in \mathbb{N}}$, the optimal rate of fixed-length source-coding is given by:

$$R_{sc}(\hat{\rho}) := \lim_{\varepsilon \rightarrow 0} \liminf_{n \rightarrow \infty} \frac{1}{n} m^{(1),\varepsilon}(\rho_n).$$

- (ii) The noisy dense coding capacity for an arbitrary sequence of bipartite states $\hat{\rho}_{AB} := \{\rho_{AB}^n\}_{n \in \mathbb{N}}$ is given by:

$$C_{dc}(\hat{\rho}_{AB}) := \lim_{\varepsilon \rightarrow 0} \limsup_{n \rightarrow \infty} \frac{1}{n} C_{dc}^{(1),\varepsilon}(\rho_{AB}^n).$$

- (iii) The distillable entanglement for an arbitrary sequence of bipartite pure states $\hat{\psi}_{AB} := \{\psi_{AB}^n\}_{n \in \mathbb{N}}$ is given by:

$$E_D(\hat{\psi}_{AB}) := \lim_{\varepsilon \rightarrow 0} \limsup_{n \rightarrow \infty} \frac{1}{n} E_D^{(1),\varepsilon}(\psi_{AB}^n).$$

- (iv) The entanglement cost of an arbitrary sequence of bipartite pure states $\hat{\psi}_{AB} := \{\psi_{AB}^n\}_{n \in \mathbb{N}}$ is given by:

$$E_C(\hat{\psi}_{AB}) := \lim_{\varepsilon \rightarrow 0} \liminf_{n \rightarrow \infty} \frac{1}{n} E_C^{(1),\varepsilon}(\psi_{AB}^n).$$

Theorems 5.5, 5.10, 5.14, 5.17 and 5.23, lead to the following results, which were originally derived in [33, 21, 6, 7, 8]:

Proposition 6.2. For the sequences $\hat{\rho}$, $\hat{\rho}_{AB}$ and $\hat{\psi}_{AB}$ given as in Definition 6.1, the following results hold:

- (i) $R_{sc}(\hat{\rho}) = \overline{S}(\hat{\rho})$
- (ii) Let $\hat{\Lambda} = \{\Lambda_n\}_{n \in \mathbb{N}}$ denote a sequence of CPTP maps $\Lambda_n : \mathcal{D}(\mathcal{H}_A^{\otimes n}) \rightarrow \mathcal{D}(\mathcal{H}_A^{\otimes n})$, $\hat{\sigma} = \{\sigma_{AB}^n\}_{n \in \mathbb{N}}$ a sequence of states with $\sigma_{AB}^n := (\Lambda_n \otimes \text{id}_{B^n}) \rho_{AB}^n$, and $d = \dim \mathcal{H}_A$. Then,
$$C_{dc}(\hat{\rho}_{AB}) = \log d - \min_{\hat{\Lambda}} \overline{S}(A|B)_{\hat{\sigma}}.$$
- (iii) Let $\hat{\rho}_A = \{\rho_A^n\}_{n \in \mathbb{N}}$ be a sequence of states with $\rho_A^n = \text{Tr}_{B^n} \psi_{AB}^n$, the partial trace being over the Hilbert spaces $\mathcal{H}_B^{\otimes n}$. Then,

$$E_D(\hat{\psi}_{AB}) = \underline{S}(\hat{\rho}_A) \quad \text{and} \quad E_C(\hat{\psi}_{AB}) = \overline{S}(\hat{\rho}_A).$$

Conclusion

We obtain second order asymptotic expansions for optimal rates of information-processing tasks in the i.i.d. setting, including fixed-length quantum source coding, noisy dense coding, and pure-state entanglement conversions. To do this, we first obtain one-shot bounds for these protocols in terms of quantities derived from the *information spectrum relative entropies*. These are two variants of the quantity (of the same name) defined in [47], which have the particular advantage of satisfying the data-processing inequality. We obtain second order asymptotic expansions for these quantities via the bounds relating them to the hypothesis testing relative entropy, and the second order asymptotic expansion of the latter derived in [47].

We recover the known second order asymptotics of *classical* fixed-length source coding (obtained by Hayashi [19]) from our corresponding quantum results. Our results for the entanglement conversions provide a refinement of the inefficiency of these protocols. We also prove that the difference in the second order asymptotics of distillable entanglement and entanglement cost results in irreversibility of entanglement concentration proved in [28].

Furthermore, we recover the known results for the optimal rates for these protocols in the more general setting of the Information Spectrum Approach (ISA) from our one-shot results. This is facilitated by the fact that the spectral divergence rates (which are the central quantities of the ISA) can be readily obtained from our information spectrum relative entropies in the asymptotic limit, when the parameter $0 < \varepsilon < 1$ (on which they depend) is taken to zero.

The information spectrum relative entropies can be used for obtaining one-shot bounds and second order asymptotics for various other tasks, but we leave the analysis of these for future research.

Acknowledgements

We are grateful to Matthias Christandl, Masahito Hayashi and Richard Jozsa for useful suggestions. We would also like to thank Ben Derrett, Christoph Harrach and Mark Wilde for helpful discussions and comments.

References

- [1] H. Barnum, C. Caves, C. Fuchs, R. Jozsa, and B. Schumacher, *On quantum coding for ensembles of mixed states*, Journal of Physics A: Mathematical and General **34** (2001), no. 35, 6767.

- [2] H. Barnum, C. Fuchs, R. Jozsa, and B. Schumacher, *General fidelity limit for quantum channels*, Physical Review A **54** (1996), no. 6, 4707.
- [3] S. Beigi and A. Gohari, *Quantum achievability proof via collision relative entropy*, arXiv:1312.3822 [quant-ph] (2013).
- [4] C. Bennett, H. Bernstein, S. Popescu, and B. Schumacher, *Concentrating partial entanglement by local operations*, Physical Review A **53** (1996), no. 4, 2046.
- [5] G. Bowen and N. Datta, *Beyond i.i.d. in quantum information theory*, Proceedings 2006 IEEE International Symposium in Information Theory (2006), 451.
- [6] G. Bowen and N. Datta, *Quantum coding theorems for arbitrary sources, channels and entanglement resources*, arXiv:quant-ph/0610003 (2006).
- [7] G. Bowen and N. Datta, *Asymptotic entanglement manipulation of bipartite pure states*, IEEE Transactions on Information Theory **54** (2008), no. 8, 3677–3686.
- [8] G. Bowen and N. Datta, *Entanglement cost for sequences of arbitrary quantum states*, Journal of Physics A: Mathematical and Theoretical **44** (2011), no. 4, 045302.
- [9] N. Datta, *Min- and max-relative entropies and a new entanglement monotone*, IEEE Transactions on Information Theory **55** (2009), no. 6, 2816–2826.
- [10] N. Datta and M.-H. Hsieh, *The apex of the family tree of protocols: Optimal rates and resource inequalities*, New Journal of Physics **13** (2011), no. 9, 093042.
- [11] N. Datta, M. Mosonyi, M.-H. Hsieh, and F.G.S.L. Brandao, *A smooth entropy approach to quantum hypothesis testing and the classical capacity of quantum channels*, IEEE Transactions on Information Theory **59** (2013), no. 12, 8014–8026.
- [12] N. Datta and R. Renner, *Smooth Rényi entropies and the quantum information spectrum*, IEEE Transactions on Information Theory **55** (2009), no. 6.
- [13] W. Feller, *An introduction to probability theory and its applications*, 2nd ed., John Wiley and Sons, 1971.
- [14] C. A Fuchs and J. Van De Graaf, *Cryptographic distinguishability measures for quantum-mechanical states*, IEEE Transactions on Information Theory **45** (1999), no. 4, 1216–1227.
- [15] T. Han and S. Verdú, *Approximation theory of output statistics*, IEEE Transactions on Information Theory **39** (1993), no. 3, 752–772.
- [16] A. Harrow and H.-K. Lo, *A tight lower bound on the classical communication cost of entanglement dilution*, IEEE Transactions on Information Theory **50** (2004), no. 2, 319–327.
- [17] M. Hayashi, *Exponents of quantum fixed-length pure-state source coding*, Physical Review A **66** (2002), 032321.
- [18] M. Hayashi, *General formulas for fixed-length quantum entanglement concentration*, IEEE Transactions on Information Theory **52** (2006), no. 5, 1904–1921.
- [19] M. Hayashi, *Second-order asymptotics in fixed-length source coding and intrinsic randomness*, IEEE Transactions on Information Theory **54** (2008), no. 10, 4619–4637.

- [20] M. Hayashi, *Information spectrum approach to second-order coding rate in channel coding*, IEEE Transactions on Information Theory **55** (2009), no. 11, 4947–4966.
- [21] M. Hayashi and H. Nagaoka, *General formulas for capacity of classical-quantum channels*, IEEE Transactions on Information Theory **49** (2003), no. 7, 1753–1768.
- [22] A.S. Holevo, *The capacity of the quantum channel with general signal states*, IEEE Transactions on Information Theory **44** (1998), no. 1, 269–273.
- [23] A.S. Holevo, *Probabilistic and statistical aspects of quantum theory*, vol. 1, Springer, 2011.
- [24] M. Horodecki, *Limits for compression of quantum information carried by ensembles of mixed states*, Physical Review A **57** (1998), no. 5, 3364.
- [25] M. Horodecki, P. Horodecki, R. Horodecki, D. Leung, and B. Terhal, *Classical capacity of a noiseless quantum channel assisted by noisy entanglement*, Quantum Information and Computation **1** (2001), no. 3, 70–78.
- [26] R. König, R. Renner, and C. Schaffner, *The operational meaning of min-and max-entropy*, IEEE Transactions on Information Theory **55** (2009), no. 9, 4337–4347.
- [27] V. Kostina and S. Verdú, *Nonasymptotic noisy lossy source coding*, IEEE Information Theory Workshop (ITW), 2013, pp. 1–5.
- [28] W. Kumagai and M. Hayashi, *Entanglement concentration is irreversible*, Physical Review Letters **111** (2013), 130407.
- [29] W. Kumagai and M. Hayashi, *Second order asymptotics for random number generation*, 2013 IEEE International Symposium on Information Theory Proceedings (ISIT), IEEE, 2013, pp. 1506–1510.
- [30] K. Li, *Second order asymptotics for quantum hypothesis testing*, Annals of Statistics **42** (2014), no. 1, 171–189.
- [31] H.-K. Lo and S. Popescu, *Concentrating entanglement by local actions: Beyond mean values*, Physical Review A **63** (2001), no. 2, 022301.
- [32] W. Matthews and S. Wehner, *Finite blocklength converse bounds for quantum channels*, arXiv:1210.4722 [quant-ph] (2012).
- [33] H. Nagaoka and M. Hayashi, *An information-spectrum approach to classical and quantum hypothesis testing for simple hypotheses*, IEEE Transactions on Information Theory **53** (2007), no. 2, 534–549.
- [34] M. Nielsen, *Conditions for a class of entanglement transformations*, Physical Review Letters **83** (1999), no. 2, 436.
- [35] M. Nielsen and J. Kempe, *Separable states are more disordered globally than locally*, Physical Review Letters **86** (2001), 5184–5187.
- [36] T. Ogawa and H. Nagaoka, *Strong converse to the quantum channel coding theorem*, IEEE Transactions on Information Theory **45** (1999), 2486–2489.
- [37] T. Ogawa and H. Nagaoka, *Strong converse and Stein’s lemma in quantum hypothesis testing*, IEEE Transactions on Information Theory **46** (2000), no. 7, 2428–2433.

- [38] R. Renner, *Security of quantum key distribution*, Ph.D. thesis, ETH Zürich, 2005.
- [39] R. Renner and R. König, *Universally composable privacy amplification against quantum adversaries*, Theory of Cryptography, Springer, 2005, pp. 407–425.
- [40] R. Renner and S. Wolf, *Smooth Rényi entropy and applications*, IEEE International Symposium on Information Theory, 2004, pp. 233–233.
- [41] B. Schumacher, *Quantum coding*, Physical Review A **51** (1995), no. 4, 2738.
- [42] B. Schumacher, *Sending entanglement through noisy quantum channels*, Physical Review A **54** (1996), no. 4, 2614.
- [43] B. Schumacher and M. Westmoreland, *Sending classical information via noisy quantum channels*, Physical Review A **56** (1997), no. 1, 131–138.
- [44] V. Strassen, *Asymptotische Abschätzungen in Shannons Informationstheorie*, Trans. Third Prague Conf. Information Theory, 1962, pp. 689–723.
- [45] M. Tomamichel, *A framework for non-asymptotic quantum information theory*, Ph.D. thesis, ETH Zürich, 2012.
- [46] M. Tomamichel, R. Colbeck, and R. Renner, *Duality between smooth min-and max-entropies*, IEEE Transactions on Information Theory **56** (2010), no. 9, 4674–4681.
- [47] M. Tomamichel and M. Hayashi, *A hierarchy of information quantities for finite block length analysis of quantum tasks*, IEEE Transactions on Information Theory **59** (2013), no. 11, 7693–7710.
- [48] M. Tomamichel and V.Y.F. Tan, *Second-order asymptotics of classical-quantum channels*, arXiv:1308.6503 [quant-ph] (2013).
- [49] L. Wang and R. Renner, *One-shot classical-quantum capacity and hypothesis testing*, Physical Review Letters **108** (2012), no. 20, 200501.
- [50] A. Winter, *Coding theorem and strong converse for quantum channels*, IEEE Transactions on Information Theory **45** (1999), no. 7, 2481–2485.
- [51] A. Winter, *Coding theorems of quantum information theory*, arXiv:quant-ph/9907077 (1999).
- [52] A. Winter, *Scalable programmable quantum gates and a new aspect of the additivity problem for the classical capacity of quantum channels*, Journal of Mathematical Physics **43** (2002), no. 9, 4341–4352.